TRAPEZE NETWORKS

A BELDEN BRAND

v7.1 Update Course

v7.1 Update

- **New Hardware**
  - **APs:** MP-82, MP-622, MP-632
  - **Appliances:** LA-200E, RM-200 Enhancement
- **MSS**
  - Advanced Feature Licensing
  - Voice/SIP Awareness
  - Cluster Enhancements
  - LDAP Support
  - Command Auditing
  - IPSEC client for RADIUS
  - AP LED and MIB Enhancements
  - Other Updates
    - AP LED controls
    - Mesh Enhancements
    - Web Portal with Local Switching
    - Support for CA Certificate chain
    - Enhancement to Dynamic RF Blacklist

Note: CLI extracts are at the end of this PowerPoint

- **RingMaster**
  - Support for MSS features
  - Grouping and Granular Access Control
  - Single System-wide sign-in
  - Audit Trail
  - Enhanced Reports
  - Other Features
- **RingMaster Global**
  - Architecture
  - Network-wide Monitoring
  - Network-wide Search
  - Network-wide Reporting
- **SmartPass**
  - RADIUS Proxy
  - MAC Authentication
  - Real time Session Monitoring
  - Web API Enhancement
  - Other Features

New Hardware

New Hardware

- MP-82
  - New high density deployment .11n AP

- MP-622
  - New outdoor .11a/b/g AP

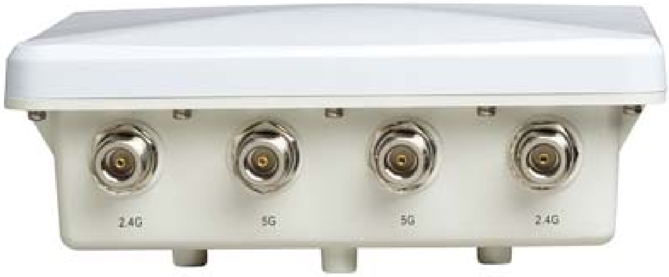
- MP-632
  - New rugged outdoor .11n AP

MP-82: Indoor .11n AP

- Intended for dense deployment
  - More APs for similar budget
  - Lower cost per AP
- Dual band 802.11n 5GHz & 2.4 GHz
  - 2x3 MIMO
  - RP-SMA connectors
- Single Ethernet port
  - 802.3af PoE
- NOT Plenum rated
- External antenna support (mid-2010)
- Mounting bracket adapter (mid-2010)
- Availability
  - Available now

MP-622: 802.11a/b/g Outdoor AP

- Replacement for MP-620
  - Provides same core features as MP-620
  - Uses same Power supply as MP-620
- Diversity antennas
  - N-type connector
- Availability
  - Mid 2010



MP-632: Outdoor 802.11n APs

- Designed for harsh environments
  - IP67/NEMA 4X
- MP-632 dual radio 802.11 5GHz & 2.4 GHz
  - Supports 3x3 MIMO
  - Six antennas ports
- Single 1000BASE-T RJ-45 port
- External hardened PS included
- Supported from MSS v7.0 MR6
- Availability
  - Available now

TRAPEZE NETWORKS
A BELDEN BRAND

LA-200E Location Appliance

- New Version of LA-200 Appliance the LA-200E
  - More Powerful (same hardware as the RM-200)
- Higher Scalability
  - Can receive data from up to 200 APs
  - Can track up to 4,000 devices
- Integrated RF-firewall Application (licensed separately)
- Future integration With RingMaster (v7.4)
- Availability
  - Available now

RM-200 Enhancement

- Automatic Backup to an External FTP/TFTP Site
- Port Bonding
  - Enable port bonding allows second port as backup
- Remote Authentication via RADIUS
  - Utilize Access Control feature in RM v7.1
- Commonly used HTML pages published to the platform page

MSS v7.1 Features & Enhancements

MSS v7.1 Topics

- Advanced Feature Licensing
- Voice/SIP Awareness
- Cluster Enhancements
- LDAP Support
- Command Auditing
- IPSEC client for RADIUS
- AP LED and MIB Enhancements
- Other Updates
  - Mesh Enhancements
  - Web Portal with Local Switching
  - Enhancement to Dynamic RF Blacklist
  - Support for CA Certificate chain

Advanced Feature Licensing

- Licenses loaded onto and applied to the MXs to enable support for these advanced features
  - **High Availability license:** enable Cluster configuration
  - **Advanced Voice license:** enable advanced voice capabilities
- Licenses loaded onto the MX to enable advanced feature support for the specified count of APs
  - **Mesh/Bridging license:** enable Mesh and bridging between APs
    - Mesh/Bridging AP increments: 4, 12, 32
  - **WAPI license:** enable WAPI & other China-specific features (China only)
    - WAPI AP increments: 4, 12, 32, 64, 128
- ***'Grandfathering'* License Deadline**
  - Customers that already use the v7.1 Clustering or Mesh features have until ***31st March 2010*** to request free licenses to allow continuing support for these features from the Web page at:

    [***http://www.trapezenetworks.com/support/product_licenses/***](http://www.trapezenetworks.com/support/product_licenses/)
  - There is a *'set'* command on the MXs to load these licenses and a *'show'* command to list the installed licenses

    Note: see CLI examples at the end of this PowerPoint

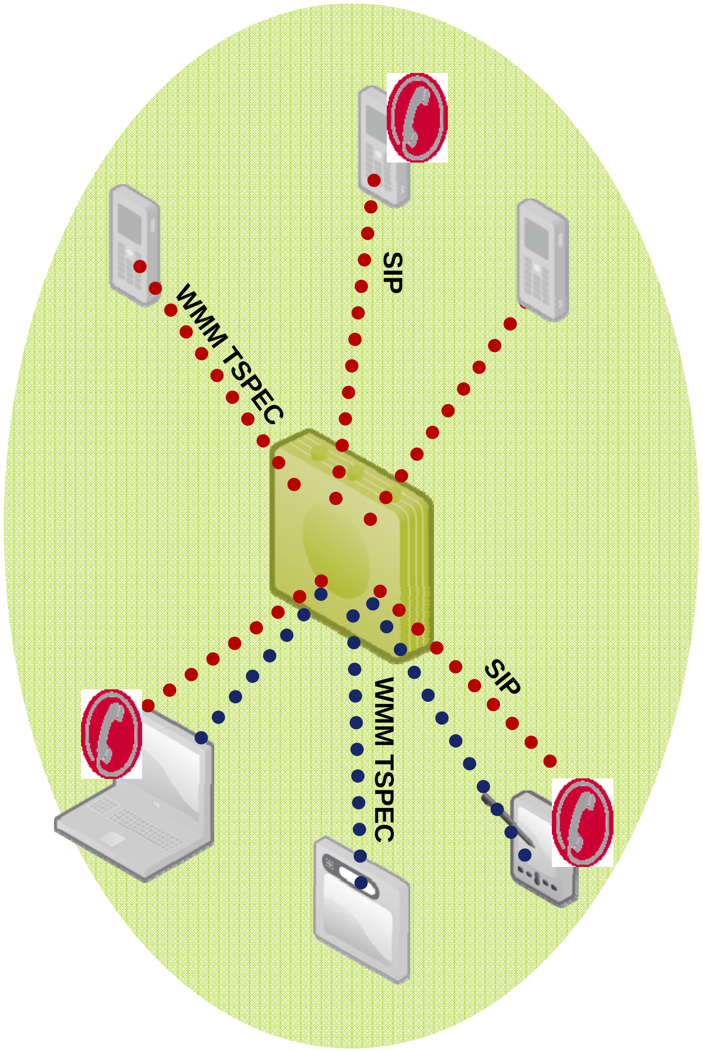
Advanced Feature Licensing Examples

- Advanced Voice License
  - Purchased for each MX that is to support the advanced voice capabilities
- High Availability License
  - Purchased for each MX that is to participate in a Cluster
  - E.g. Licenses required for a cluster of 2 x MX-200R supporting 128 APs
    - **2 x MX-2xx-U32:** to provide support for 64 additional APs
    - **2 x MX-2xx-HA-LIC:** to enable clustering on both MXs
  - E.g. Licenses required for a cluster of 2 x MX-2800 supporting 512 APs
    - **2 x MX-2800-U64:** } to provide support
    - **2 x MX-2800-U128:** } for 384 additional APs
    - **2 x MX-22800-HA-LIC:** to enable clustering on both MXs

      Note: Customers only need to purchase AP licenses for the actual number of APs being deployed in the Cluster
- Mesh/Bridging License
  - Purchased for each AP that is to support the Mesh or Bridging capabilities
    - License must be installed on the Seed MXs of a Cluster system
    - License must be installed on each MX that has the configuration for the mesh/bridge APs (High or Low Bias)

Voice/SIP Awareness

- Stateful protocol inspection at the AP
  - Regardless of the switching model (central or local)
- Dynamic Call Admission Control (CAC)
  - preserves voice call quality through coordinated bandwidth reservations
- Visibility into SIP session state with QoS for detected SIP flows
- Call detail records
- SIP-aware, ACLs, QoS-profiles, and packet marking work together to classify packets in either direction
  - Packets on Ethernet are classified and marked with 802.1p and DSCP *‘Expedited Forwarding’* per hop behavior
  - Packets on the radio are classified and marked in the WMM header

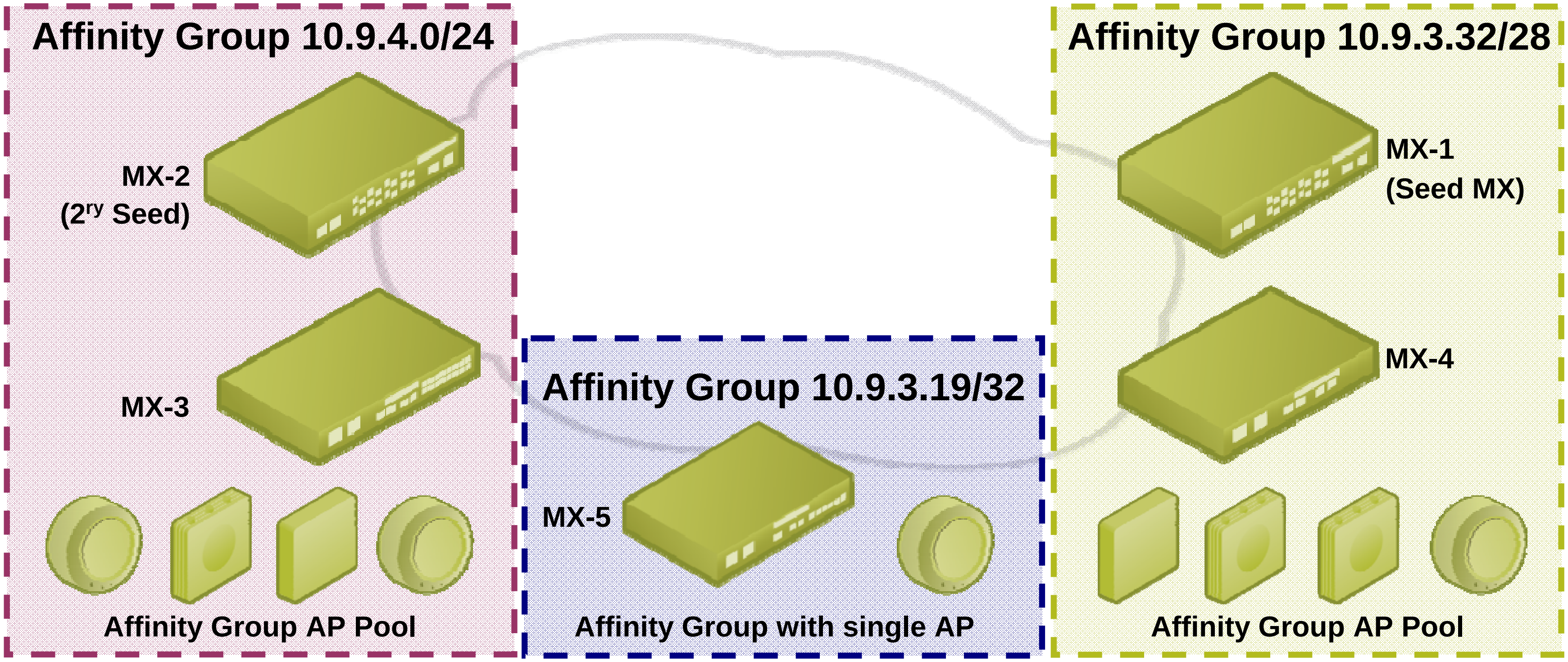


Voice/SIP Awareness Details

- QOS-Profile
  - A v7.1 QoS-profile can set the CoS for a ***'traffic class'***
    - A traffic class is a kind of predefined traffic filter
    - *'voip-data'* is the only traffic-class defined in v7.1
  - Traffic-class ***'voip-data'*** sets QoS policy for packets of an active SIP call
    - To the specified CoS and max bandwidth values
    - All other packets get the QoS policy specified on the QoS-profile
  - The ***'max-bw'*** parameter for *'voip-data'* provides 2 features
    - It limits the bandwidth of a single voice call
    - It uses TSPEC emulation based on the client bandwidth and data rate to maximize system voice capacity
  - The most specific policy is applied on a per packet basis
- A roaming client with an active SIP call is always supported
- SIP control packets are automatically given video priority (CoS 5)

Cluster AP Affinity Groups

- AP Affinity Groups can be defined to specify a ***preferred PAM*** for a specific pool of APs specified by a CIDR-like variable length Subnet mask (VLSM)
  - SAMs are chosen from a non Affinity Group MX or a ***different*** Affinity Group
  - Affinity Groups are specified on the Cluster Seed MX and associated to the appropriate member MXs

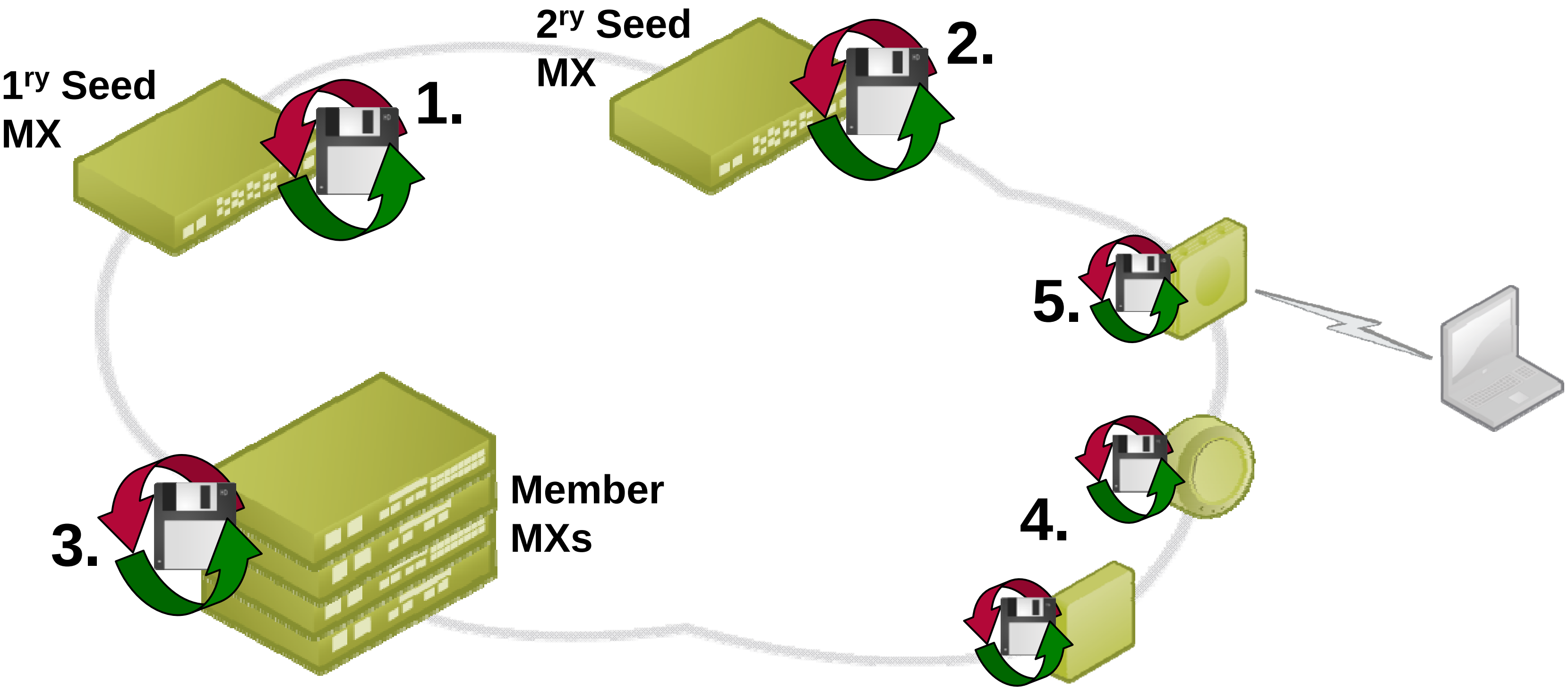


Affinity Group 10.9.4.0/24
MX-2
(2ry Seed)
MX-3
Affinity Group AP Pool
Affinity Group 10.9.3.19/32
MX-5
Affinity Group with single AP
Affinity Group 10.9.3.32/28
MX-1
(Seed MX)
MX-4
Affinity Group AP Pool

Cluster In-Service Upgrade

- Hitless upgrade of the SW on the Cluster MXs and APs
  - A secondary Seed MUST be available on the Cluster
  - All MXs must be at and upgraded to the same SW version
  - Upgrade order: **1.** Primary Seed **2.** Secondary Seed **3.** Member MXs **4.** & **5.** APs

    Note: APs are upgraded where possible with no impact to connected users



Other Cluster Enhancements

- Additions to the Cluster configuration settings
  - RADIUS/LDAP configuration
  - System and Network Access rules
  - Global 802.1X configuration settings

  Note: these items are no longer available on the individual cluster members
- Scalability Improvements
  - MX-2800 scaled to 512 APs and 12,800 clients

LDAP Support

- LDAPv3 AAA support for:
  - Web Portal authentication
  - Console access
  - Telnet & SSH access
  - MAC authentication
- Supported Operations
  - Authentication ONLY
  - *‘bindRequest’* | *‘bindResponse’* | *‘unbindRequest’*
  - No support for search or admin proxy search operations
- Configurable LDAP server groups
  - LDAP server configuration is part of the Cluster configuration
  - For redundancy and load balancing
  - Configurable server timeouts
- Configuration Interfaces
  - RingMaster and CLI only (not available via WebView)
- Interoperable with leading directory servers

Command Auditing

- Log all CLI commands to an external server for auditing purposes
  - All commands which complete successfully are logged
  - Commands may be logged to an external RADIUS server
  - The enable password is obscured
  - Configuration is handled as an additional RADIUS accounting type
    - VSA 13
  - Each accounting command message contains:
    - Timestamp
    - tty port
    - Username
    - Source IP address
    - Command issued
    - Command status (success/failure)

Note: Incorrect commands are not logged

IPSEC for Radius

- Basic IPSEC support in MSS only (no RingMaster support)
  - Static key for encryption and authentication (no IKE)
  - Transport mode with encryption between the IP source and destination addresses
  - Encapsulating Security Payload (ESP) mechanism
  - Encryption ciphers available: AES, 3DES
  - Integrity checking using HMAC-SHA1*
- The IPSEC tunnel must be established between an MX and RADIUS server before RADIUS communications are started
- The RADIUS server must support IPSec
  - A RADIUS server is considered an IPSec *'Peer'*
  - A maximum of 16 peers are supported

* Hash-based Message Authentication Code – Secure Hash Algorithm 1

AP LED and MIB Enhancements

- AP LED Control
  - Allow the customer to set the LED behavior on an AP by AP basis
  - The LED setting becomes active after the AP receives its configuration
  - LEDs may be set in three ways:
    - **Auto** (default): LEDS behave in Trapeze standard way
    - **Static:** LEDS do not flash when traffic flows (all other LED behavior is as normal)
    - **Off:** All LEDs are off once the AP is active
  - A range of APs may be set at the same time
- AP MIBs
  - Provides more complete AP configuration MIB information
    - AP Configuration Table: indexed by AP Number
    - Radio configuration Table: indexed by AP Number, Radio Number
    - Radio Profiles Table: indexed by Radio Profile Name
    - Service Profile Table connected to Radio Profile: indexed by Radio and Sevice Profile Names
    - Snoop Filters connected to Radio Profile
    - AP Unconfigured MIB: AP Table indexed by AP Serial Number
    - Auto-AP Template

Other MSS Features

- Mesh Enhancements
  - Multi hop Bridging is now supported
  - Bridging and Mesh can now support 802.11n data rates
- Local Switching Extended to support Web Portal
- Enhancement to Dynamic RF Blacklist
  - Administrative add clients to the RF blacklist
  - Ability to exclude clients from automatic entry into the list
- Support for multiple CA certificates (Chains)
- Scheduled Command Execution
  - Schedule by: Date/Time, Frequency, System Start/Shutdown
  - Run a script file stored within the MX’s file system

Other MSS Features

- Other improvements
  - Authenticate admin HTTPs requests via AAA
  - *‘Service-type’* based Access to Privileged CLI mode
  - Wired authentication idle session timeout
  - Ad-hoc Countermeasures
  - Trap Log MIB
  - 802.1X TKIP/CCMP Rekey Timers
  - Mixed cipher support
  - Configurable RM communications port
  - SCP for secure file transfer
  - TFTP Daemon

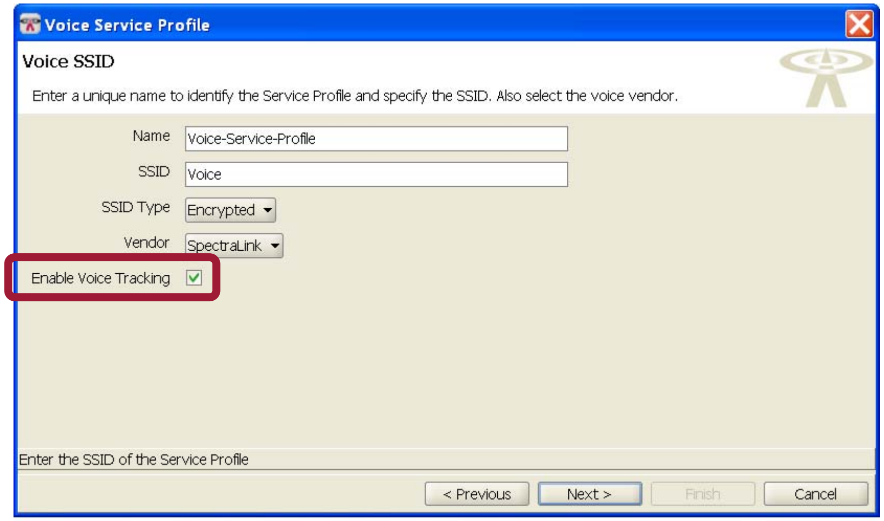
Ringmaster v7.1 Features & Enhancements

RingMaster v7.1 Topics

- Support for MSS features:
  - Voice/SIP Awareness
  - Cluster Enhancements
  - LDAP Support
- Grouping and Granular Access Control
- Single System-wide sign-in
- Audit Trail
- Enhanced Reports
- Other Features
  - Monitoring improvements
  - AP and Session scaling
  - Client Blacklist and countermeasures enhancements
  - Server certificate management
  - Configurable MX TLS port

SIP Awareness & Monitoring

- Voice Service Profile
  - **Step 1:** User starts Voice Service Wizard and enables stateful inspection of Voice protocols



Voice SSID

Enter a unique name to identify the Service Profile and specify the SSID. Also select the voice vendor.

Name: Voice-Service-Profile

SSID: Voice

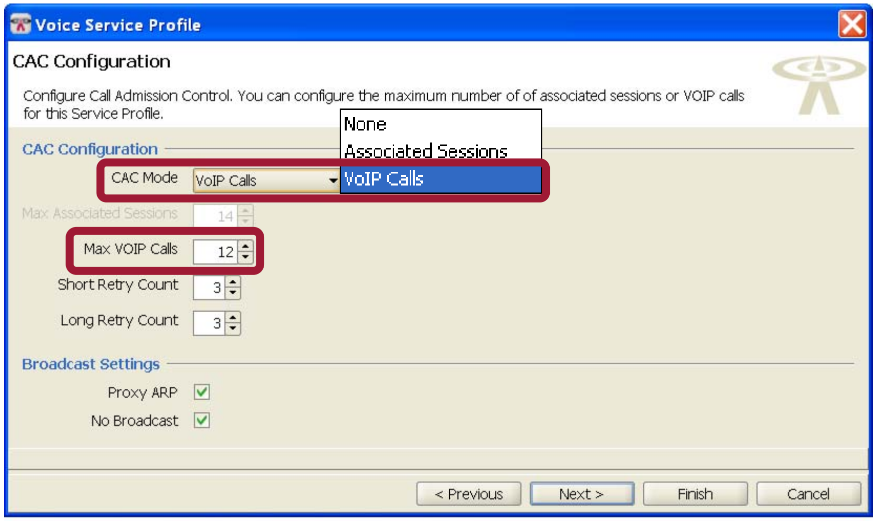
SSID Type: Encrypted

Vendor: SpectraLink

Enable Voice Tracking ☑

Enter the SSID of the Service Profile

  - **Step 2:** User configures Voice Call Admission Control, specifying the number of allowed active calls.



CAC Configuration

Configure Call Admission Control. You can configure the maximum number of of associated sessions or VOIP calls for this Service Profile.

CAC Configuration

CAC Mode: VoIP Calls

Max Associated Sessions: 14

Max VOIP Calls: 12

Short Retry Count: 3

Long Retry Count: 3

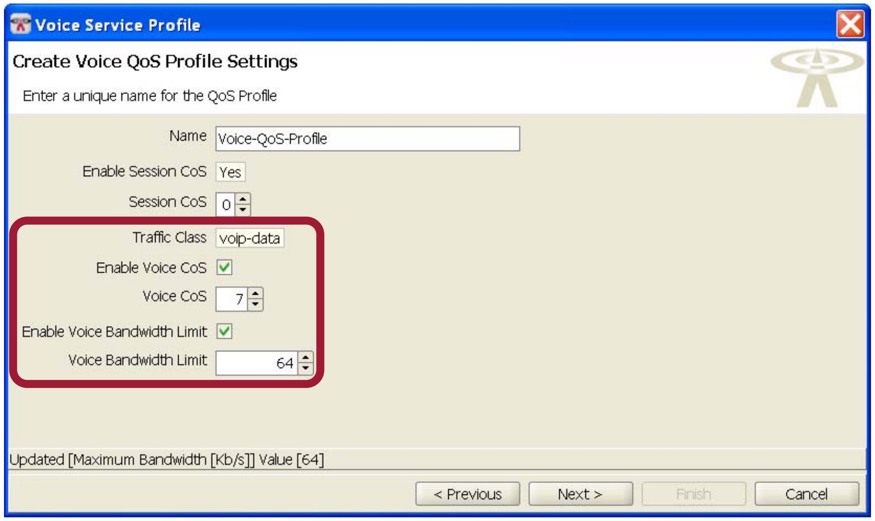
Broadcast Settings

Proxy ARP ☑

No Broadcast ☑

SIP Awareness & Monitoring

- Voice Service Profile
  - **Step 3:** User configures QoS settings for the identified Voice flows (CoS and Max-BW).



Create Voice QoS Profile Settings

Enter a unique name for the QoS Profile

Name: Voice-QoS-Profile

Enable Session CoS: Yes

Session CoS: 0

Traffic Class: voip-data

Enable Voice CoS: ☑

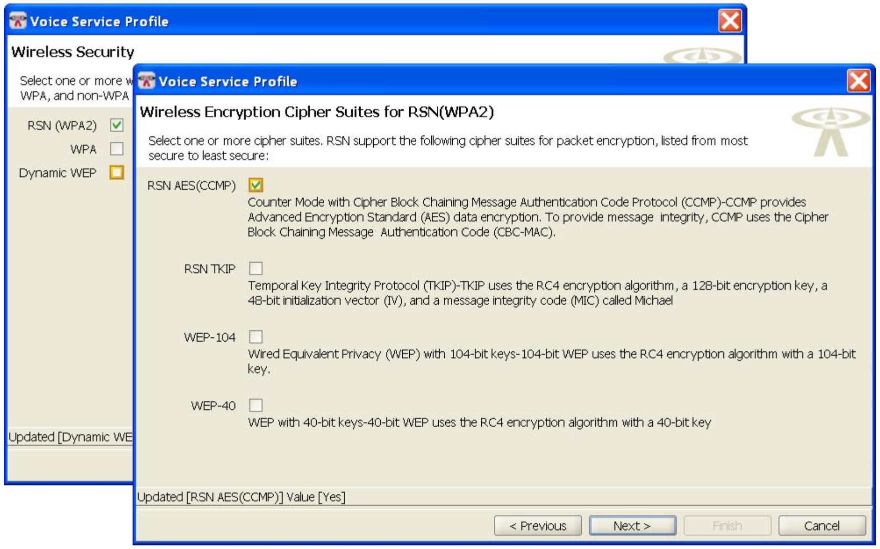
Voice CoS: 7

Enable Voice Bandwidth Limit: ☑

Voice Bandwidth Limit: 64

Updated [Maximum Bandwidth [Kb/s]] Value [64]

  - **Step 4:** User completes wizard by supplying standard SSID information i.e. security settings, VLAN configuration, etc…



Wireless Security

Select one or more w
WPA, and non-WPA

RSN (WPA2) ☑

WPA □

Dynamic WEP □

Updated [Dynamic WE

Wireless Encryption Cipher Suites for RSN(WPA2)

Select one or more cipher suites. RSN support the following cipher suites for packet encryption, listed from most secure to least secure:

RSN AES(CCMP) ☑
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)-CCMP provides Advanced Encryption Standard (AES) data encryption. To provide message integrity, CCMP uses the Cipher Block Chaining Message Authentication Code (CBC-MAC).

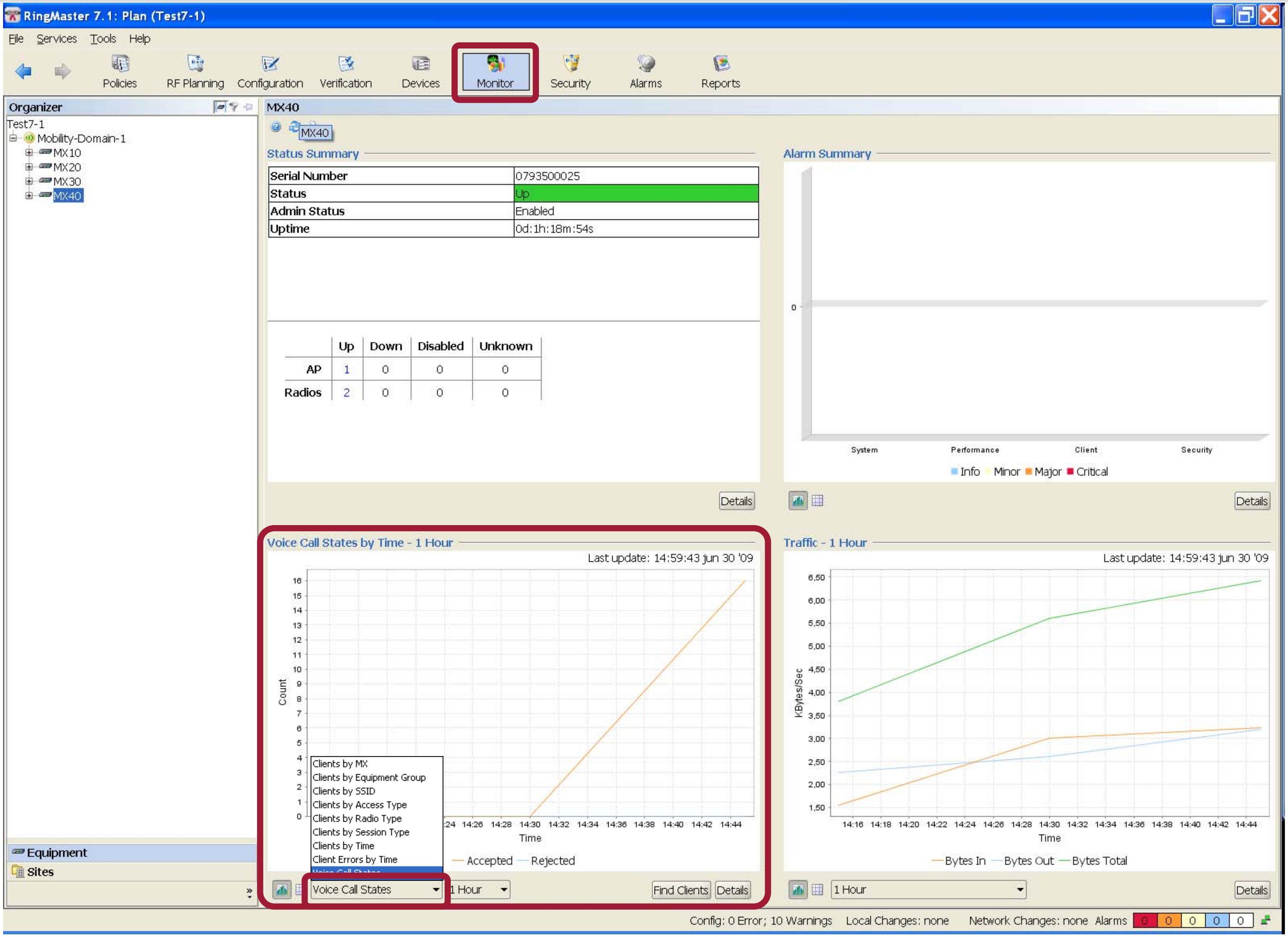
RSN TKIP □
Temporal Key Integrity Protocol (TKIP)-TKIP uses the RC4 encryption algorithm, a 128-bit encryption key, a 48-bit initialization vector (IV), and a message integrity code (MIC) called Michael

WEP-104 □
Wired Equivalent Privacy (WEP) with 104-bit keys-104-bit WEP uses the RC4 encryption algorithm with a 104-bit key.

WEP-40 □
WEP with 40-bit keys-40-bit WEP uses the RC4 encryption algorithm with a 40-bit key

Updated [RSN AES(CCMP)] Value [Yes]

Voice Monitoring Features



RingMaster 7.1: Plan (Test7-1)

MX40

Status Summary

Serial Number	0793500025
Status	Up
Admin Status	Enabled
Uptime	0d:1h:18m:54s

	Up	Down	Disabled	Unknown
AP	1	0	0	0
Radios	2	0	0	0

Alarm Summary

Voice Call States by Time - 1 Hour

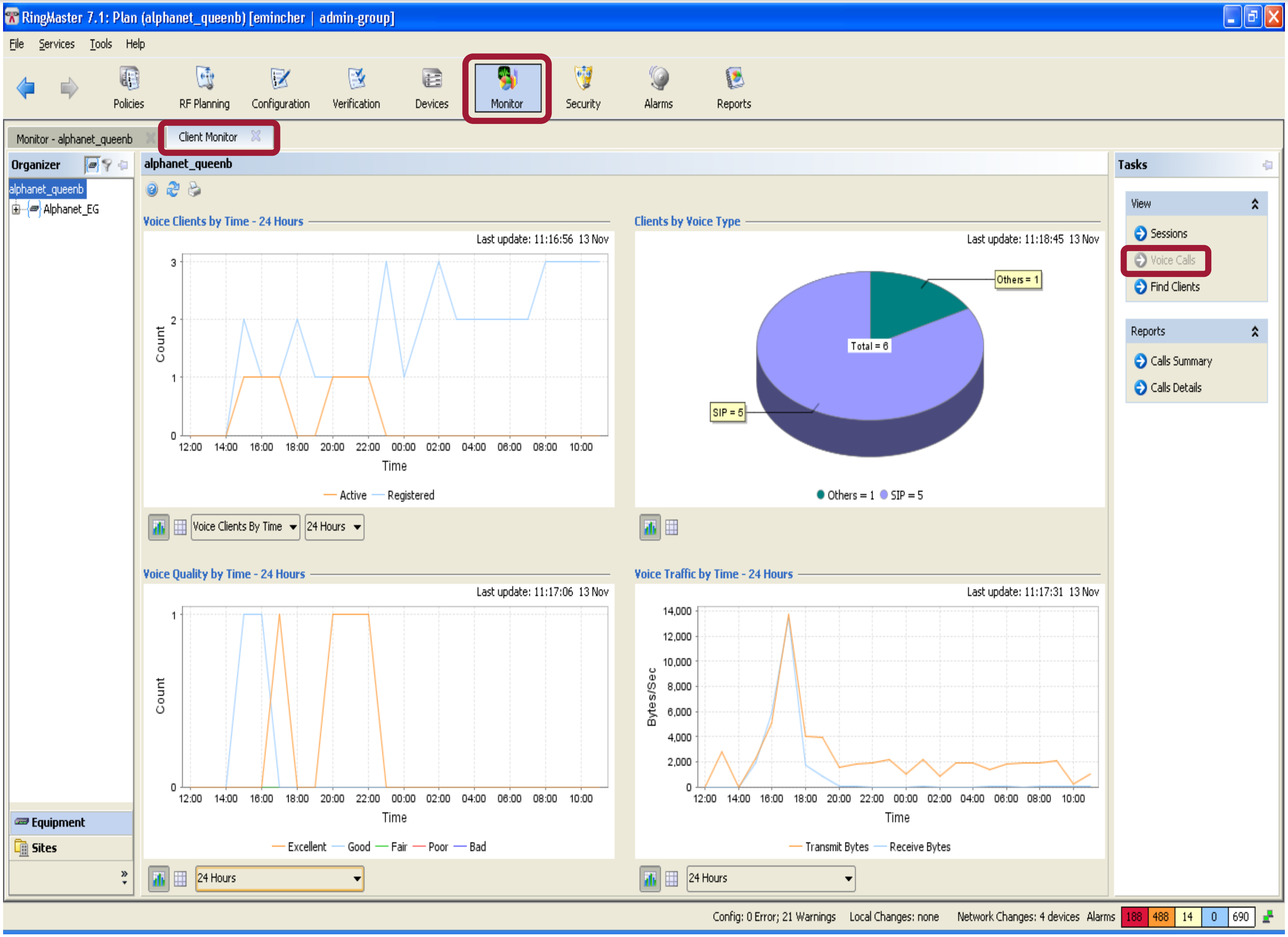
Last update: 14:59:43 Jun 30 '09

Traffic - 1 Hour

Last update: 14:59:43 Jun 30 '09

Config: 0 Error; 10 Warnings Local Changes: none Network Changes: none Alarms 0 0 0 0 0

Voice Specific Monitoring Panel

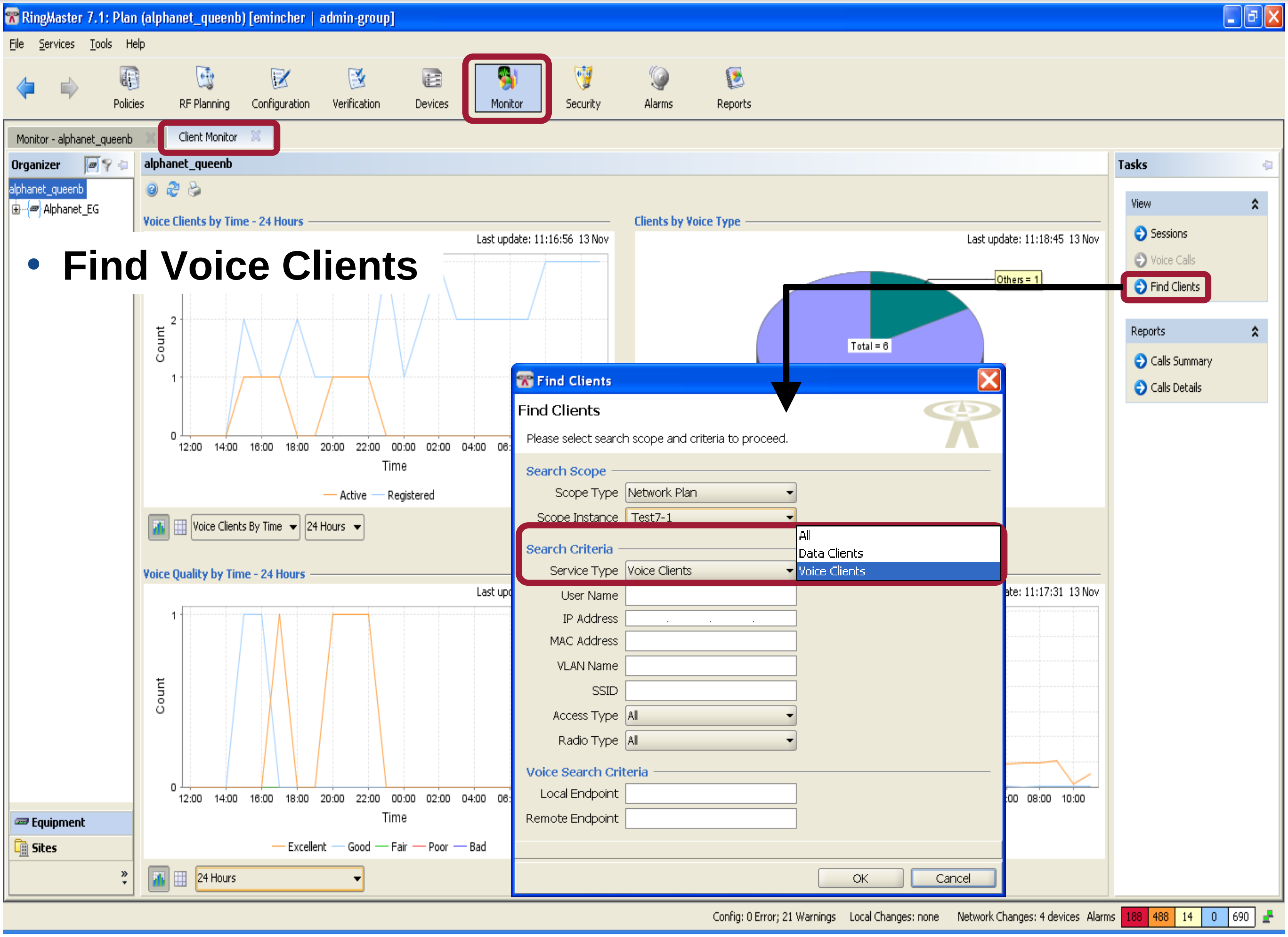


RingMaster 7.1: Plan (alphanet_queenb) [emincher | admin-group]

Config: 0 Error; 21 Warnings Local Changes: none Network Changes: 4 devices Alarms 188 488 14 0 690

Troubleshoot Voice Clients – 1

- **Find Voice Clients**



Find Clients

Please select search scope and criteria to proceed.

Search Scope

Scope Type: Network Plan

Scope Instance: Test7-1

Search Criteria

Service Type: Voice Clients

- All
- Data Clients
- Voice Clients

User Name:

IP Address: . . .

MAC Address:

VLAN Name:

SSID:

Access Type: All

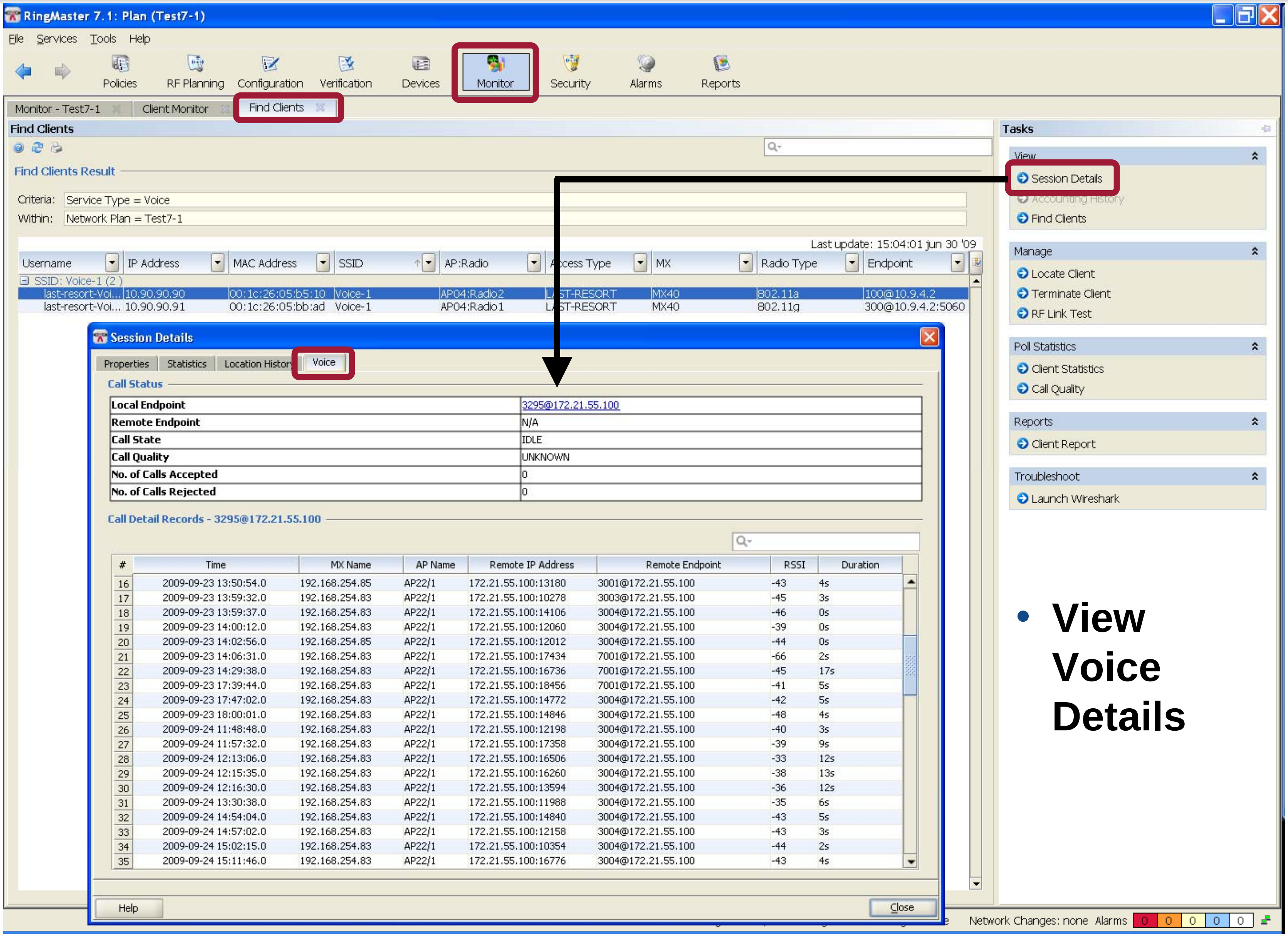
Radio Type: All

Voice Search Criteria

Local Endpoint:

Remote Endpoint:

Troubleshoot Voice Clients – 2



Find Clients

Find Clients Result

Criteria: Service Type = Voice

Within: Network Plan = Test7-1

Last update: 15:04:01 jun 30 '09

Username	IP Address	MAC Address	SSID	AP:Radio	Access Type	MX	Radio Type	Endpoint
SSID: Voice-1 (2)								
last-resort-Voi...	10.90.90.90	00:1c:26:05:b5:10	Voice-1	AP04:Radio2	LAST-RESORT	MX40	802.11a	100@10.9.4.2
last-resort-Voi...	10.90.90.91	00:1c:26:05:bb:ad	Voice-1	AP04:Radio1	LAST-RESORT	MX40	802.11g	300@10.9.4.2:5060

Session Details

Call Status

Local Endpoint	3295@172.21.55.100
Remote Endpoint	N/A
Call State	IDLE
Call Quality	UNKNOWN
No. of Calls Accepted	0
No. of Calls Rejected	0

Call Detail Records - 3295@172.21.55.100

#	Time	MX Name	AP Name	Remote IP Address	Remote Endpoint	RSSI	Duration
16	2009-09-23 13:50:54.0	192.168.254.85	AP22/1	172.21.55.100:13180	3001@172.21.55.100	-43	4s
17	2009-09-23 13:59:32.0	192.168.254.83	AP22/1	172.21.55.100:10278	3003@172.21.55.100	-45	3s
18	2009-09-23 13:59:37.0	192.168.254.83	AP22/1	172.21.55.100:14106	3004@172.21.55.100	-46	0s
19	2009-09-23 14:00:12.0	192.168.254.83	AP22/1	172.21.55.100:12060	3004@172.21.55.100	-39	0s
20	2009-09-23 14:02:56.0	192.168.254.85	AP22/1	172.21.55.100:12012	3004@172.21.55.100	-44	0s
21	2009-09-23 14:06:31.0	192.168.254.83	AP22/1	172.21.55.100:17434	7001@172.21.55.100	-66	2s
22	2009-09-23 14:29:38.0	192.168.254.83	AP22/1	172.21.55.100:16736	7001@172.21.55.100	-45	17s
23	2009-09-23 17:39:44.0	192.168.254.83	AP22/1	172.21.55.100:18456	7001@172.21.55.100	-41	5s
24	2009-09-23 17:47:02.0	192.168.254.83	AP22/1	172.21.55.100:14772	3004@172.21.55.100	-42	5s
25	2009-09-23 18:00:01.0	192.168.254.83	AP22/1	172.21.55.100:14846	3004@172.21.55.100	-48	4s
26	2009-09-24 11:48:48.0	192.168.254.83	AP22/1	172.21.55.100:12198	3004@172.21.55.100	-40	3s
27	2009-09-24 11:57:32.0	192.168.254.83	AP22/1	172.21.55.100:17358	3004@172.21.55.100	-39	9s
28	2009-09-24 12:13:06.0	192.168.254.83	AP22/1	172.21.55.100:16506	3004@172.21.55.100	-33	12s
29	2009-09-24 12:15:35.0	192.168.254.83	AP22/1	172.21.55.100:16260	3004@172.21.55.100	-38	13s
30	2009-09-24 12:16:30.0	192.168.254.83	AP22/1	172.21.55.100:13594	3004@172.21.55.100	-36	12s
31	2009-09-24 13:30:38.0	192.168.254.83	AP22/1	172.21.55.100:11988	3004@172.21.55.100	-35	6s
32	2009-09-24 14:54:04.0	192.168.254.83	AP22/1	172.21.55.100:14840	3004@172.21.55.100	-43	5s
33	2009-09-24 14:57:02.0	192.168.254.83	AP22/1	172.21.55.100:12158	3004@172.21.55.100	-43	3s
34	2009-09-24 15:02:15.0	192.168.254.83	AP22/1	172.21.55.100:10354	3004@172.21.55.100	-44	2s
35	2009-09-24 15:11:46.0	192.168.254.83	AP22/1	172.21.55.100:16776	3004@172.21.55.100	-43	4s

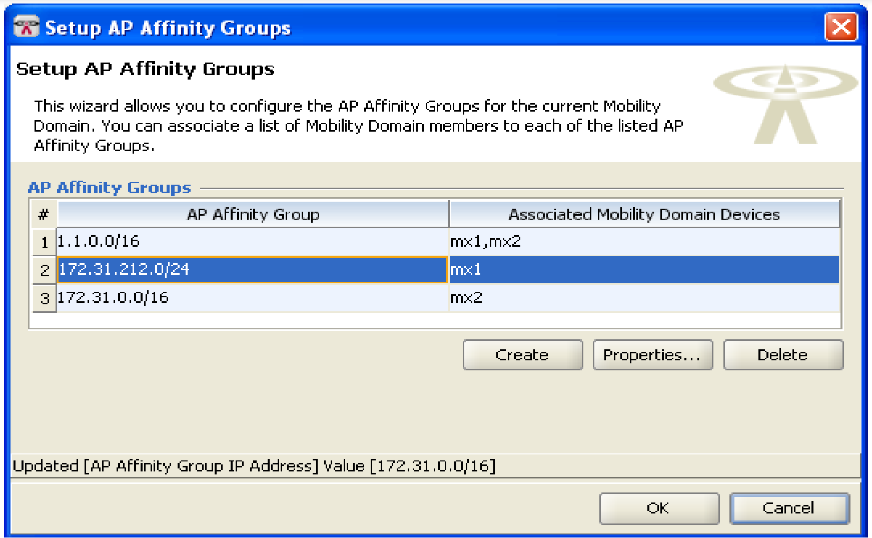
- **View Voice Details**

Voice Alarms and Call Detail Records

- Voice Alarms
  - The Alarms detail panel shows all current voice related alarms e.g.
    - Call failures
    - Active call threshold alarms
- Call Detail Records
  - Call detail records are reported via RADIUS accounting
    - Integration with SmartPass is required
  - New Voice-related Reports
    - Call Details
    - Call Summary

Cluster Enhancements

- AP Affinity Wizard
  - Specify Affinity Group by CIDR-like Variable Length Subnet Mask
  - Associate Affinity Group with appropriate MX(s)
- Cluster Upgrade Wizard
  - Manages the hitless Cluster upgrade

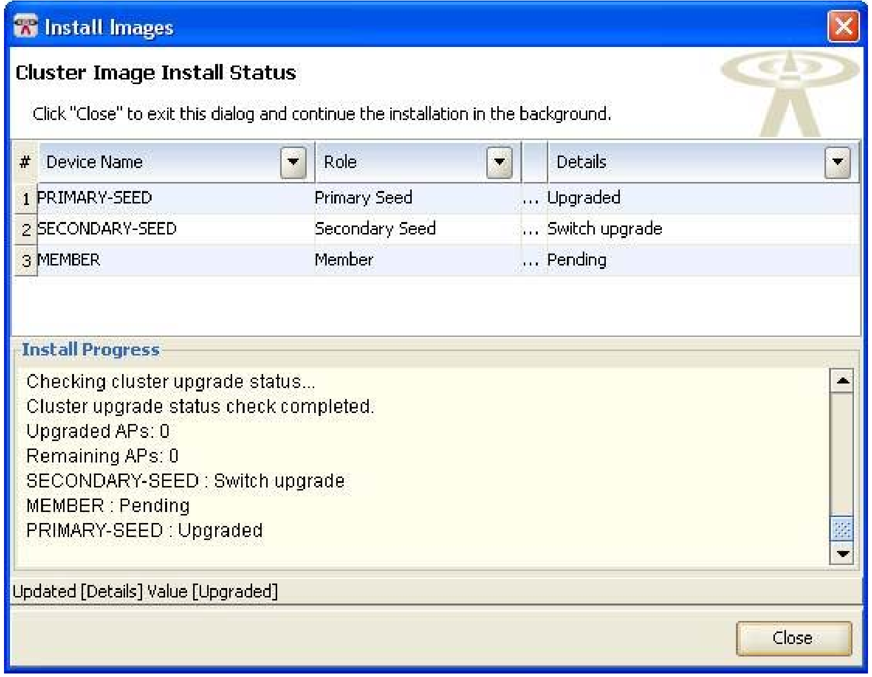


Setup AP Affinity Groups

This wizard allows you to configure the AP Affinity Groups for the current Mobility Domain. You can associate a list of Mobility Domain members to each of the listed AP Affinity Groups.

#	AP Affinity Group	Associated Mobility Domain Devices
1	1.1.0.0/16	mx1,mx2
2	172.31.212.0/24	mx1
3	172.31.0.0/16	mx2

Updated [AP Affinity Group IP Address] Value [172.31.0.0/16]



Cluster Image Install Status

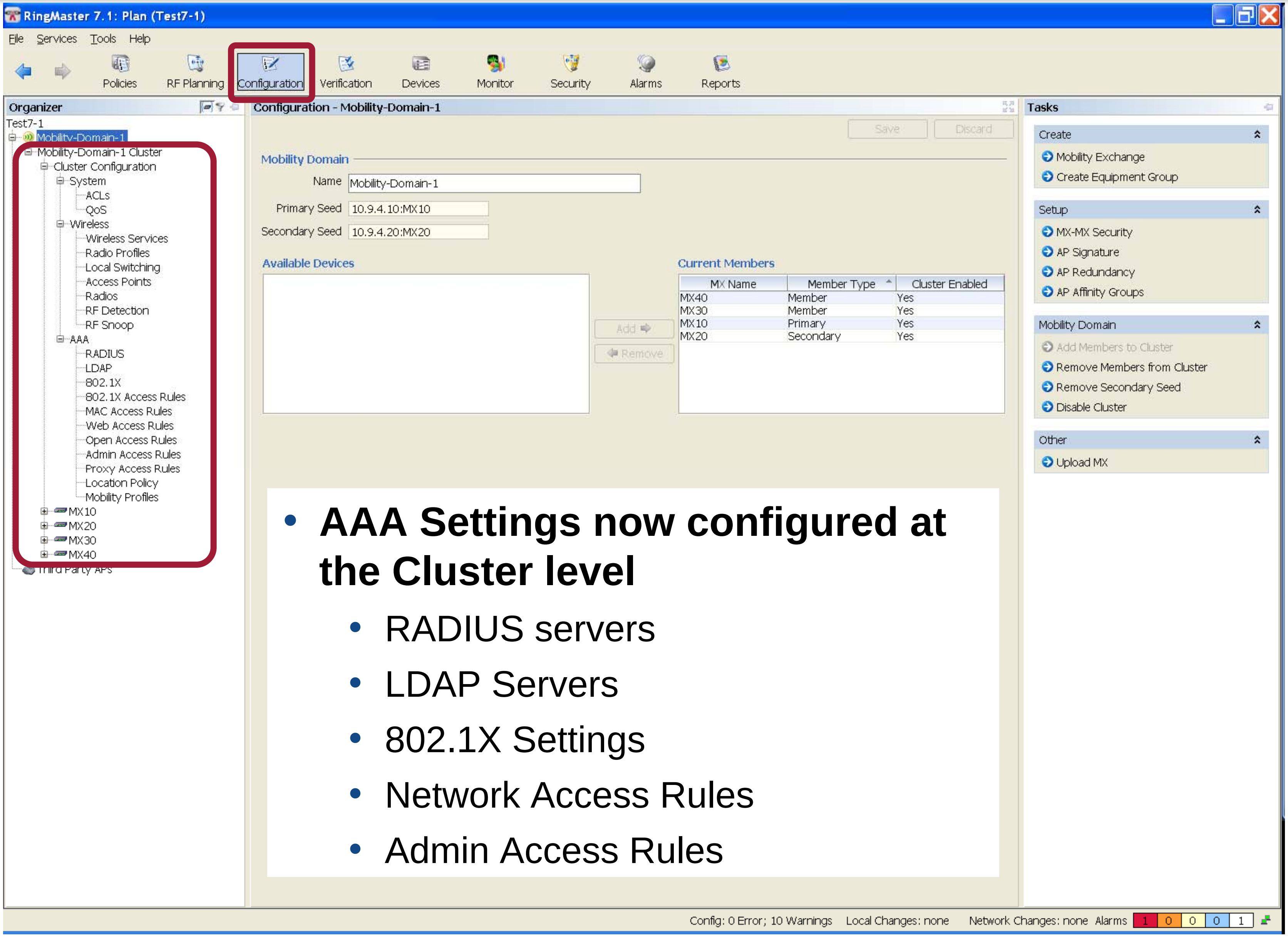
Click "Close" to exit this dialog and continue the installation in the background.

#	Device Name	Role	Details
1	PRIMARY-SEED	Primary Seed	... Upgraded
2	SECONDARY-SEED	Secondary Seed	... Switch upgrade
3	MEMBER	Member	... Pending

```
Checking cluster upgrade status...
Cluster upgrade status check completed.
Upgraded APs: 0
Remaining APs: 0
SECONDARY-SEED : Switch upgrade
MEMBER : Pending
PRIMARY-SEED : Upgraded
```

Updated [Details] Value [Upgraded]

Cluster Settings



Configuration - Mobility-Domain-1

Mobility Domain

Name: Mobility-Domain-1

Primary Seed: 10.9.4.10:MX10

Secondary Seed: 10.9.4.20:MX20

Available Devices

Current Members

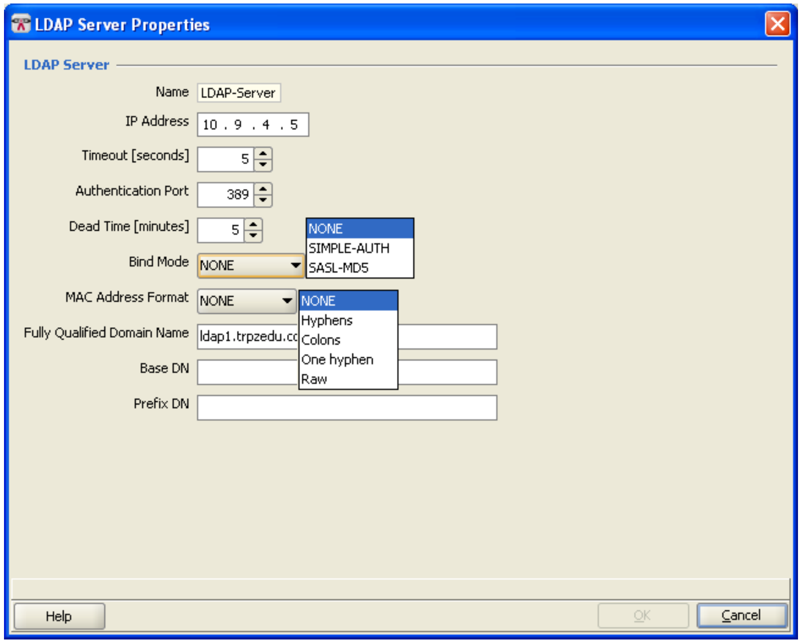
MX Name	Member Type	Cluster Enabled
MX40	Member	Yes
MX30	Member	Yes
MX10	Primary	Yes
MX20	Secondary	Yes

Config: 0 Error; 10 Warnings Local Changes: none Network Changes: none Alarms 1 0 0 0 1

- **AAA Settings now configured at the Cluster level**
  - RADIUS servers
  - LDAP Servers
  - 802.1X Settings
  - Network Access Rules
  - Admin Access Rules

LDAP Support

- LDAP support
  - Configure LDAP servers
  - Found under AAA settings on an MX or Cluster

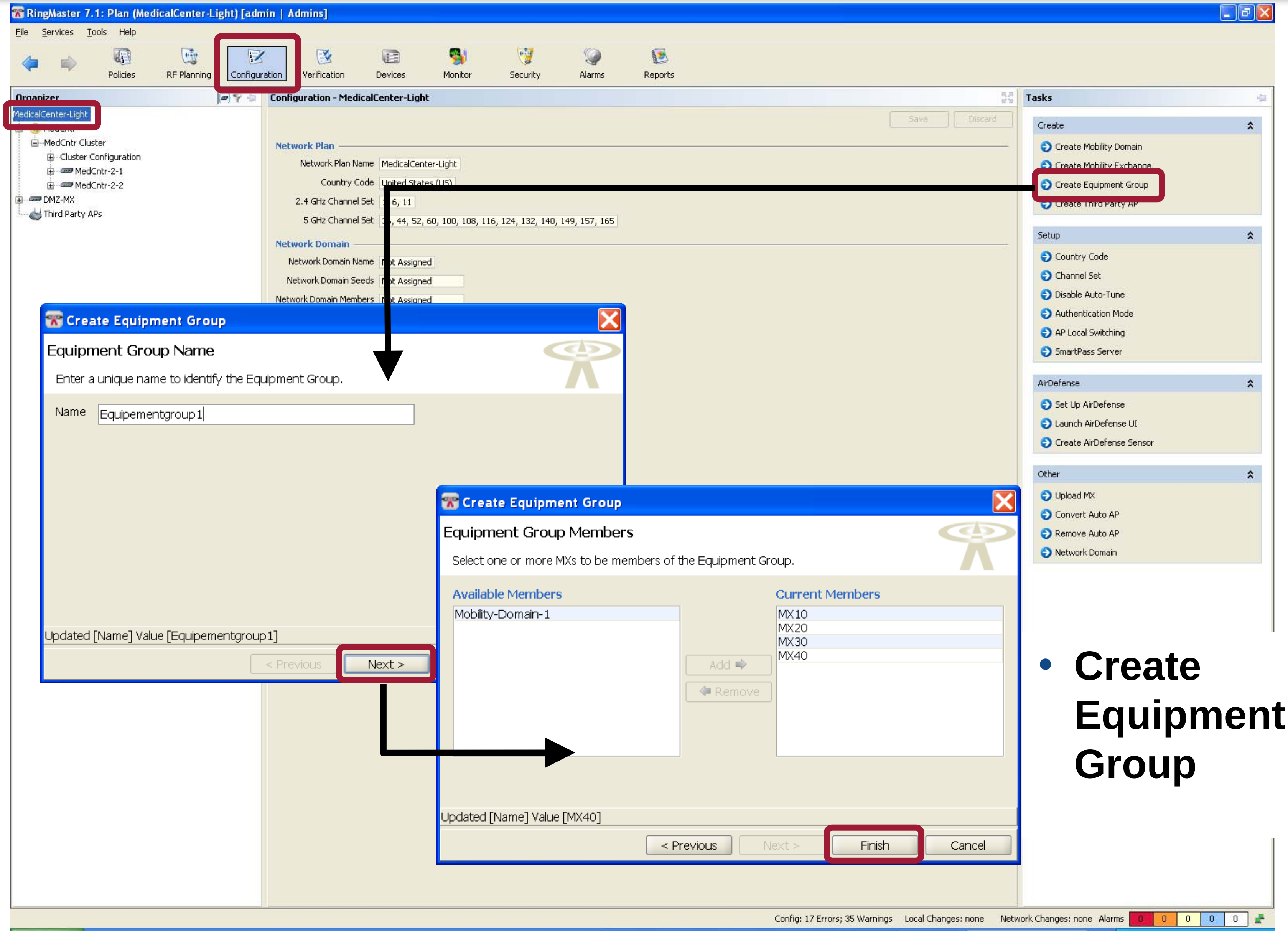


LDAP Server Properties

LDAP Server

Name	LDAP-Server
IP Address	10 . 9 . 4 . 5
Timeout [seconds]	5
Authentication Port	389
Dead Time [minutes]	5
Bind Mode	NONE
MAC Address Format	NONE
Fully Qualified Domain Name	ldap1.trpzedu.co
Base DN	
Prefix DN	

Grouping and Access Control



RingMaster 7.1: Plan (MedicalCenter-Light) [admin | Admins]

MedicalCenter-Light
- MedCntr Cluster
  - Cluster Configuration
  - MedCntr-2-1
  - MedCntr-2-2
- DMZ-MX
- Third Party APs

Configuration - MedicalCenter-Light

Network Plan

Network Plan Name: MedicalCenter-Light

Country Code: United States (US)

2.4 GHz Channel Set: 1, 6, 11

5 GHz Channel Set: 36, 44, 52, 60, 100, 108, 116, 124, 132, 140, 149, 157, 165

Network Domain

Network Domain Name: Not Assigned

Network Domain Seeds: Not Assigned

Network Domain Members: Not Assigned

Create Equipment Group

Equipment Group Name

Enter a unique name to identify the Equipment Group.

Name: Equipementgroup1

Updated [Name] Value [Equipementgroup1]

Create Equipment Group

Equipment Group Members

Select one or more MXs to be members of the Equipment Group.

Available Members: Mobility-Domain-1

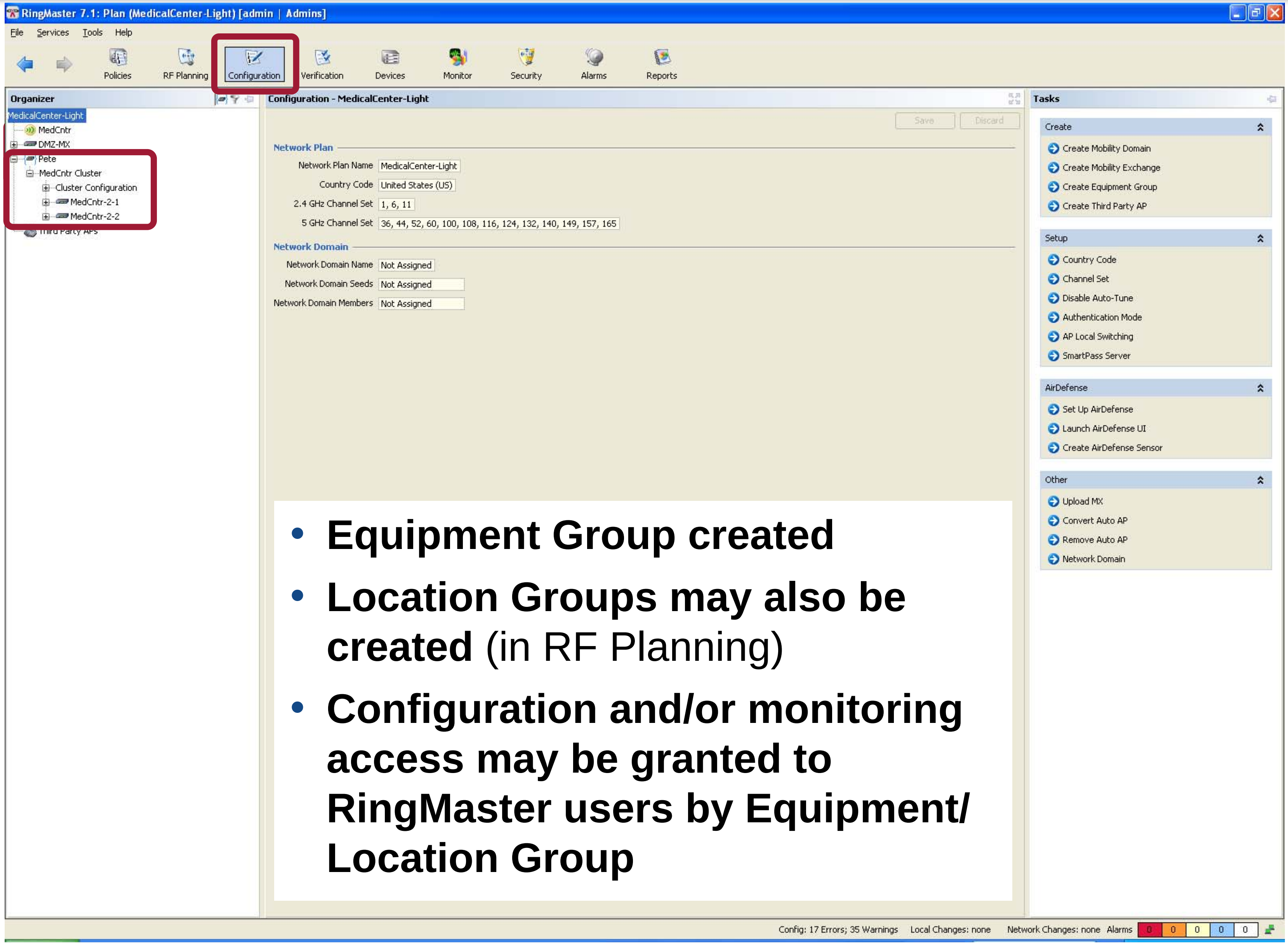
Current Members: MX10, MX20, MX30, MX40

Updated [Name] Value [MX40]

Config: 17 Errors; 35 Warnings   Local Changes: none   Network Changes: none   Alarms 0 0 0 0 0

- **Create Equipment Group**

Grouping and Access Control



Network Plan

Network Plan Name: MedicalCenter-Light

Country Code: United States (US)

2.4 GHz Channel Set: 1, 6, 11

5 GHz Channel Set: 36, 44, 52, 60, 100, 108, 116, 124, 132, 140, 149, 157, 165

Network Domain

Network Domain Name: Not Assigned

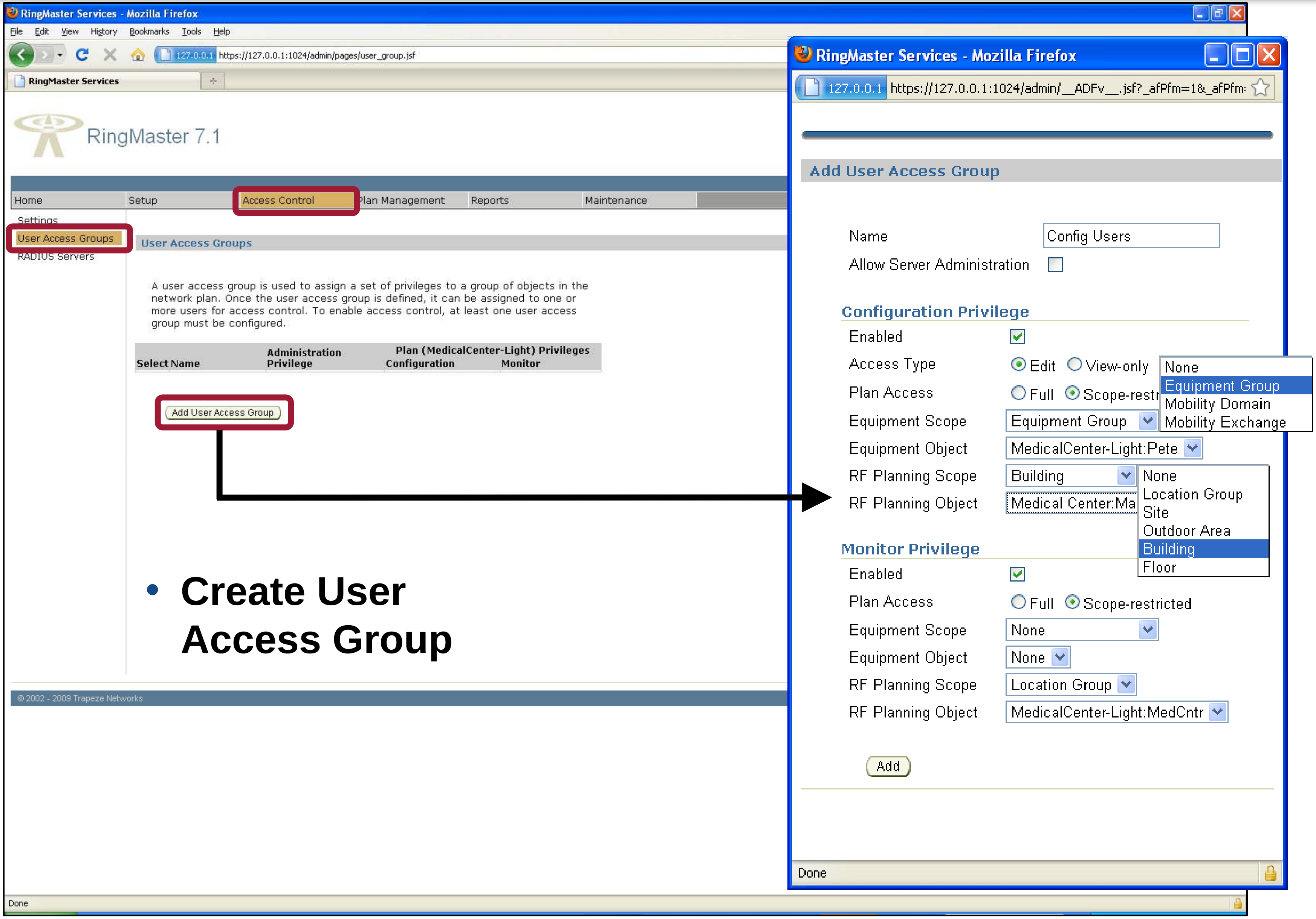
Network Domain Seeds: Not Assigned

Network Domain Members: Not Assigned

Config: 17 Errors; 35 Warnings   Local Changes: none   Network Changes: none   Alarms 0 0 0 0 0

- **Equipment Group created**
- **Location Groups may also be created** (in RF Planning)
- **Configuration and/or monitoring access may be granted to RingMaster users by Equipment/ Location Group**

Grouping and Access Control



RingMaster Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
127.0.0.1 https://127.0.0.1:1024/admin/pages/user_group.jsf
RingMaster Services
RingMaster 7.1
Home
Setup
Access Control
Plan Management
Reports
Maintenance
Settings
User Access Groups
RADIUS Servers
Add User Access Group
© 2002 - 2009 Trapeze Networks
Done
RingMaster Services - Mozilla Firefox
127.0.0.1 https://127.0.0.1:1024/admin/__ADFv__.jsf?_afPfm=1&_afPfm
Add
Done

User Access Groups

A user access group is used to assign a set of privileges to a group of objects in the network plan. Once the user access group is defined, it can be assigned to one or more users for access control. To enable access control, at least one user access group must be configured.

Select Name	Administration Privilege	Plan (MedicalCenter-Light) Privileges Configuration	 Monitor

Add User Access Group

Name: Config Users

Allow Server Administration ☐

Configuration Privilege

Enabled ☑

Access Type ● Edit ○ View-only

Plan Access ○ Full ● Scope-restr

Equipment Scope: Equipment Group (None / Equipment Group / Mobility Domain / Mobility Exchange)

Equipment Object: MedicalCenter-Light:Pete

RF Planning Scope: Building (None / Location Group / Site / Outdoor Area / Building / Floor)

RF Planning Object: Medical Center:Ma

Monitor Privilege

Enabled ☑

Plan Access ○ Full ● Scope-restricted

Equipment Scope: None

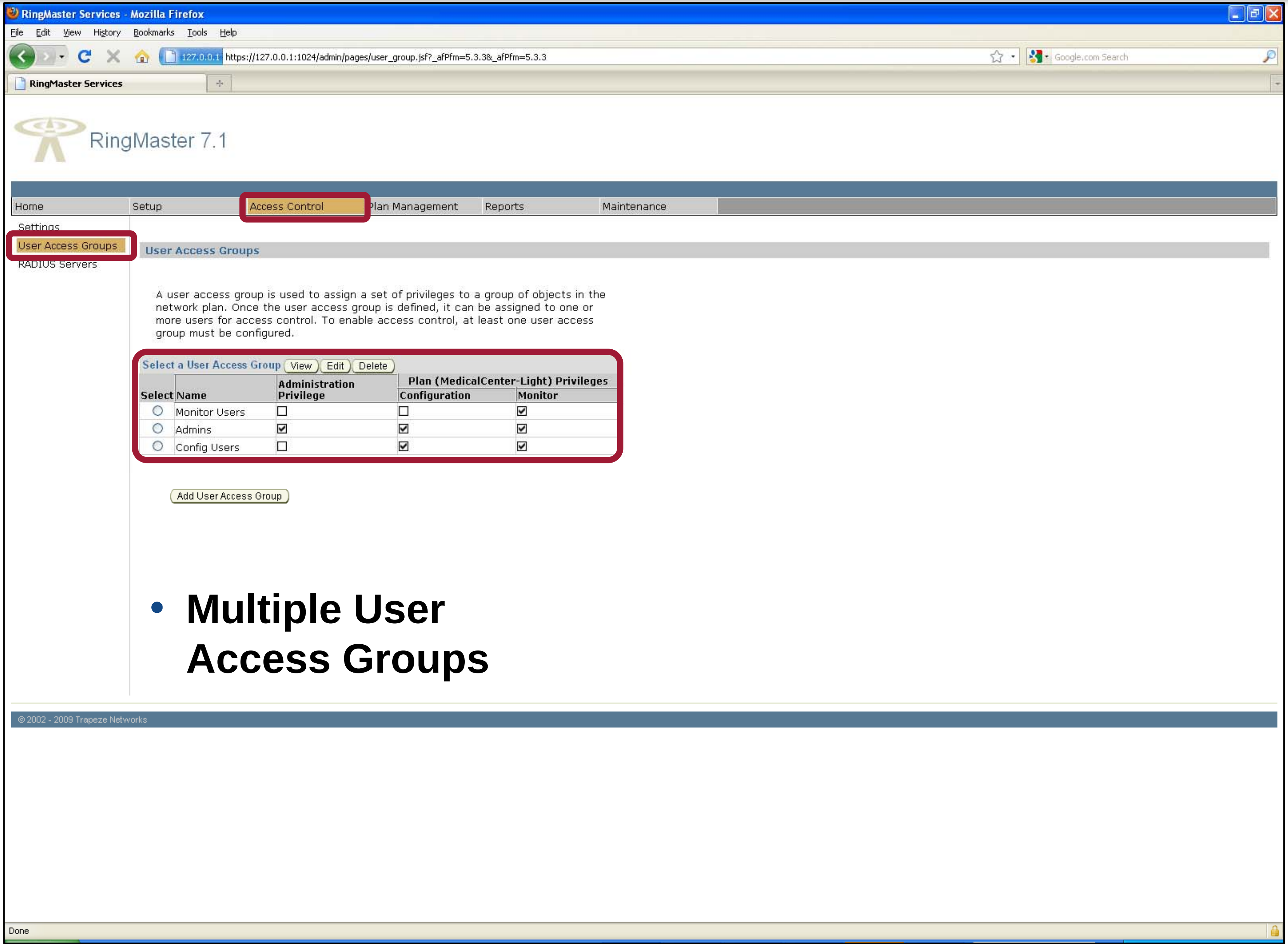
Equipment Object: None

RF Planning Scope: Location Group

RF Planning Object: MedicalCenter-Light:MedCntr

- **Create User Access Group**

Grouping and Access Control



RingMaster Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
127.0.0.1 https://127.0.0.1:1024/admin/pages/user_group.jsf?_afPfm=5.3.3&_afPfm=5.3.3
Google.com Search
RingMaster Services
RingMaster 7.1
Home
Setup
Access Control
Plan Management
Reports
Maintenance
Settings
User Access Groups
RADIUS Servers
View
Edit
Delete
Add User Access Group
© 2002 - 2009 Trapeze Networks
Done

User Access Groups

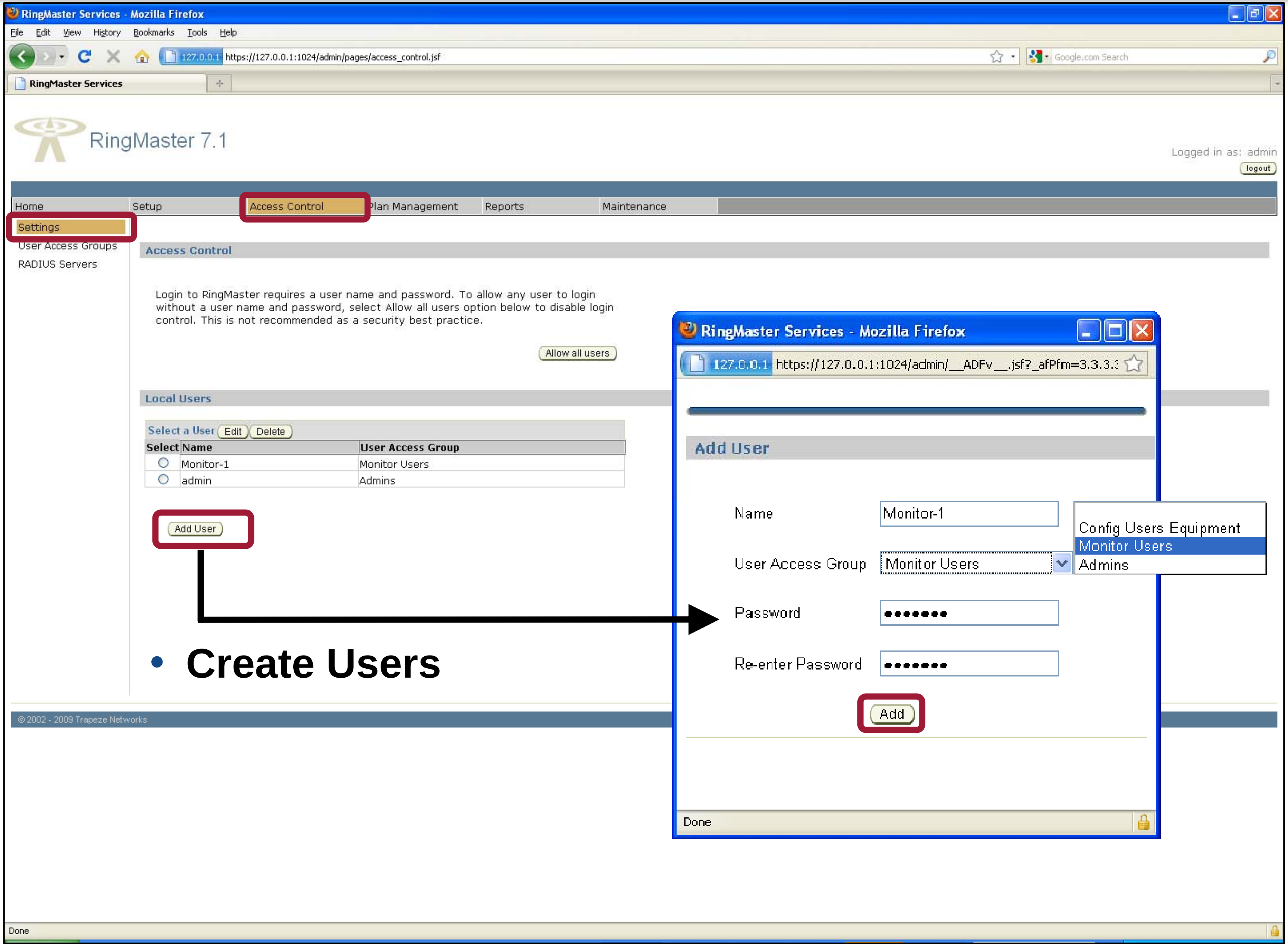
A user access group is used to assign a set of privileges to a group of objects in the network plan. Once the user access group is defined, it can be assigned to one or more users for access control. To enable access control, at least one user access group must be configured.

Select a User Access Group

Select	Name	Administration Privilege	Plan (MedicalCenter-Light) Privileges Configuration	Monitor
○	Monitor Users	□	□	☑
○	Admins	☑	☑	☑
○	Config Users	□	☑	☑

- **Multiple User Access Groups**

Grouping and Access Control



RingMaster Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
127.0.0.1 https://127.0.0.1:1024/admin/pages/access_control.jsf
Google.com Search
RingMaster Services
RingMaster 7.1
Logged in as: admin
logout
Home
Setup
Access Control
Plan Management
Reports
Maintenance
Settings
User Access Groups
RADIUS Servers

Access Control

Login to RingMaster requires a user name and password. To allow any user to login without a user name and password, select Allow all users option below to disable login control. This is not recommended as a security best practice.

Local Users

Select a User
Edit
Delete

Select	Name	User Access Group
○	Monitor-1	Monitor Users
○	admin	Admins

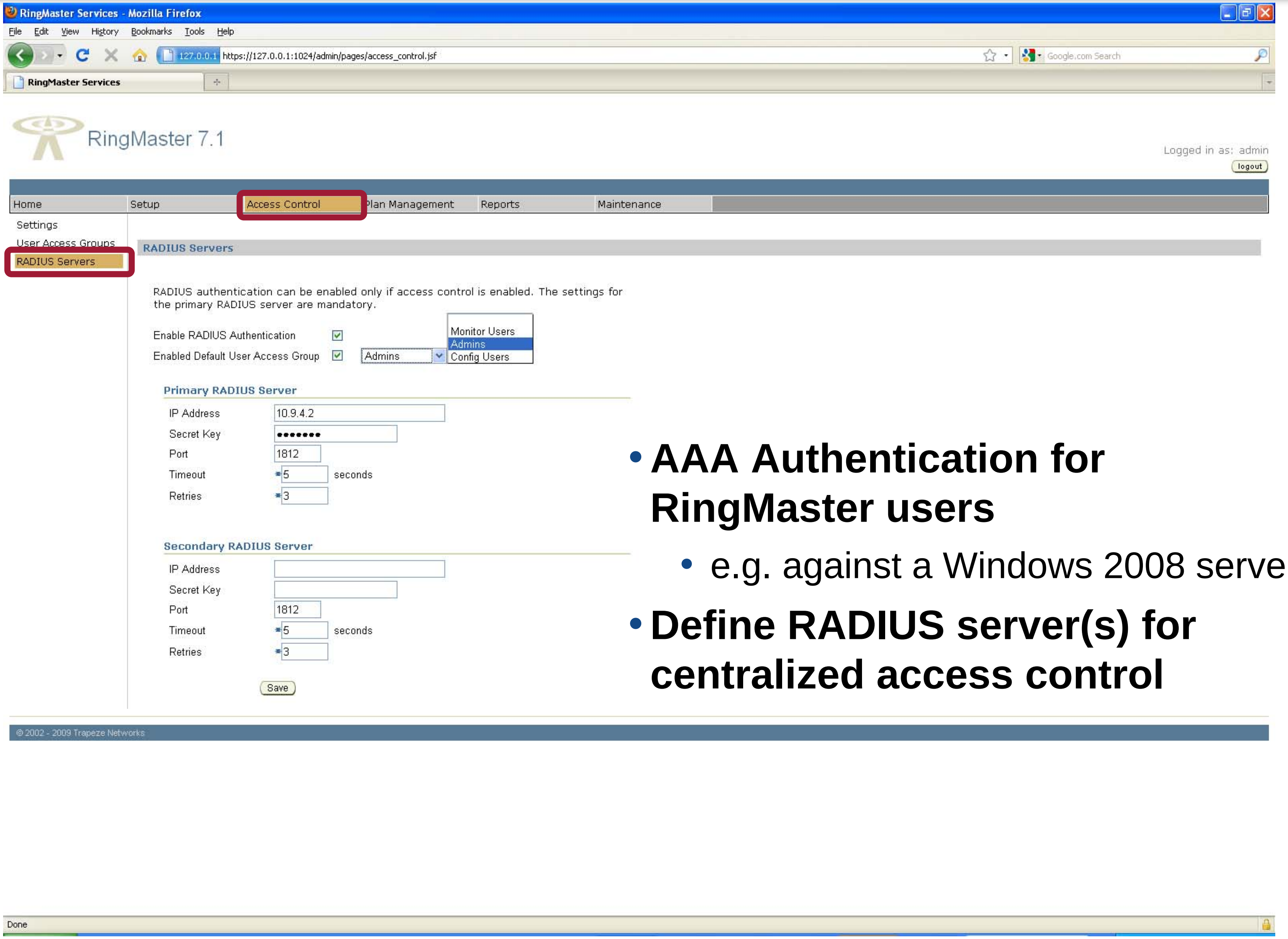
Add User
© 2002 - 2009 Trapeze Networks
Done
RingMaster Services - Mozilla Firefox
127.0.0.1 https://127.0.0.1:1024/admin/__ADFv__.jsf?_afPfm=3.3.3.3

Add User

Name	Monitor-1
User Access Group	Monitor Users
Password	●●●●●●●
Re-enter Password	●●●●●●●

- **Create Users**

Single System-wide Login


RingMaster Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://127.0.0.1:1024/admin/pages/access_control.jsf
RingMaster Services
RingMaster 7.1
Logged in as: admin
logout
Home
Setup
Access Control
Plan Management
Reports
Maintenance
Settings
User Access Groups
RADIUS Servers
Save
© 2002 - 2009 Trapeze Networks
Done

RADIUS Servers

RADIUS authentication can be enabled only if access control is enabled. The settings for the primary RADIUS server are mandatory.

Enable RADIUS Authentication ☑

Enabled Default User Access Group ☑ Admins (Monitor Users / Admins / Config Users)

Primary RADIUS Server

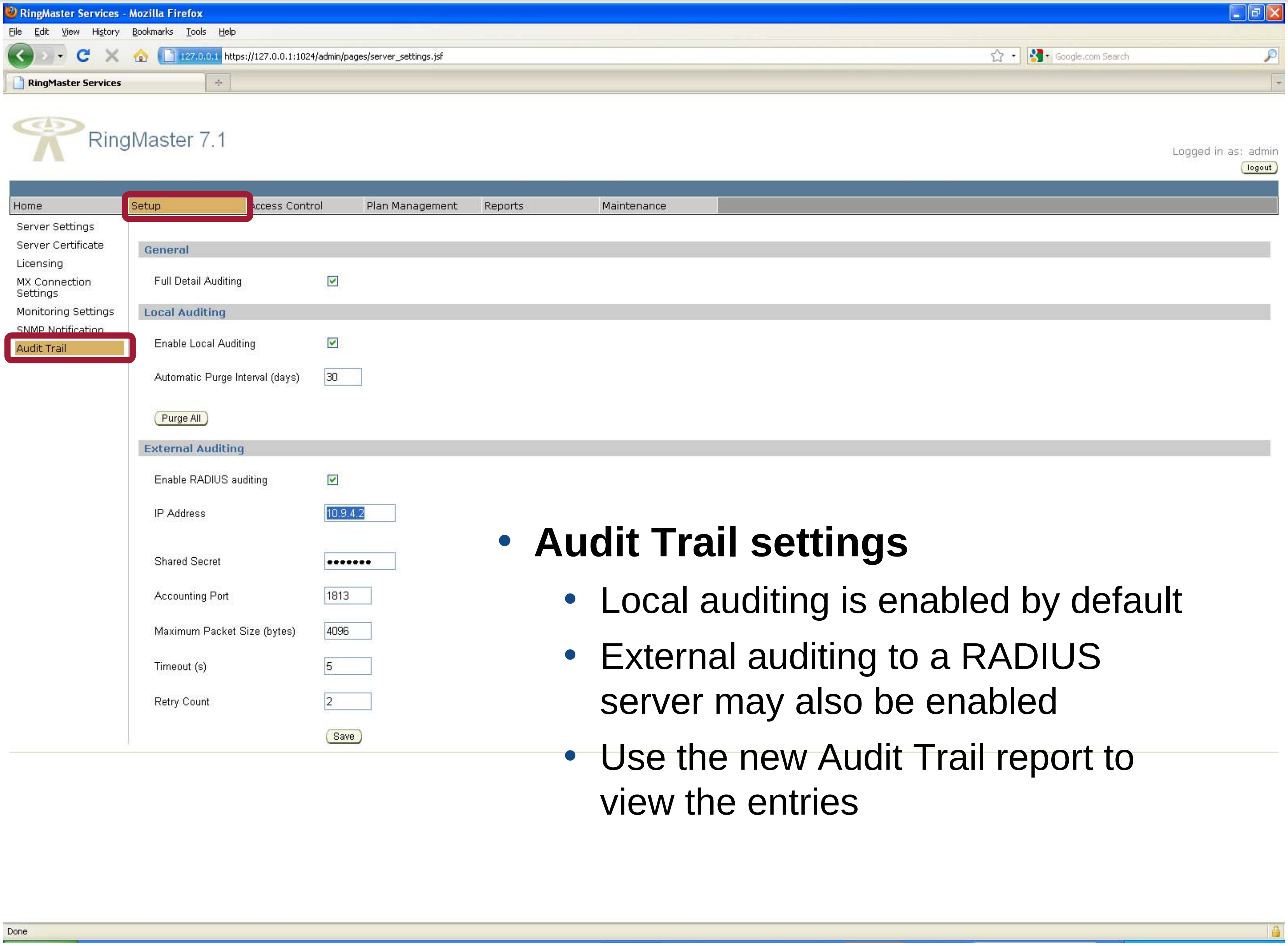
IP Address	10.9.4.2
Secret Key	•••••••
Port	1812
Timeout	5 seconds
Retries	3

Secondary RADIUS Server

IP Address	
Secret Key	
Port	1812
Timeout	5 seconds
Retries	3

- **AAA Authentication for RingMaster users**
  - e.g. against a Windows 2008 server
- **Define RADIUS server(s) for centralized access control**

Audit Trail



General

Full Detail Auditing ☑

Local Auditing

Enable Local Auditing ☑

Automatic Purge Interval (days): 30

External Auditing

Enable RADIUS auditing ☑

IP Address: 10.9.4.2

Shared Secret: •••••••

Accounting Port: 1813

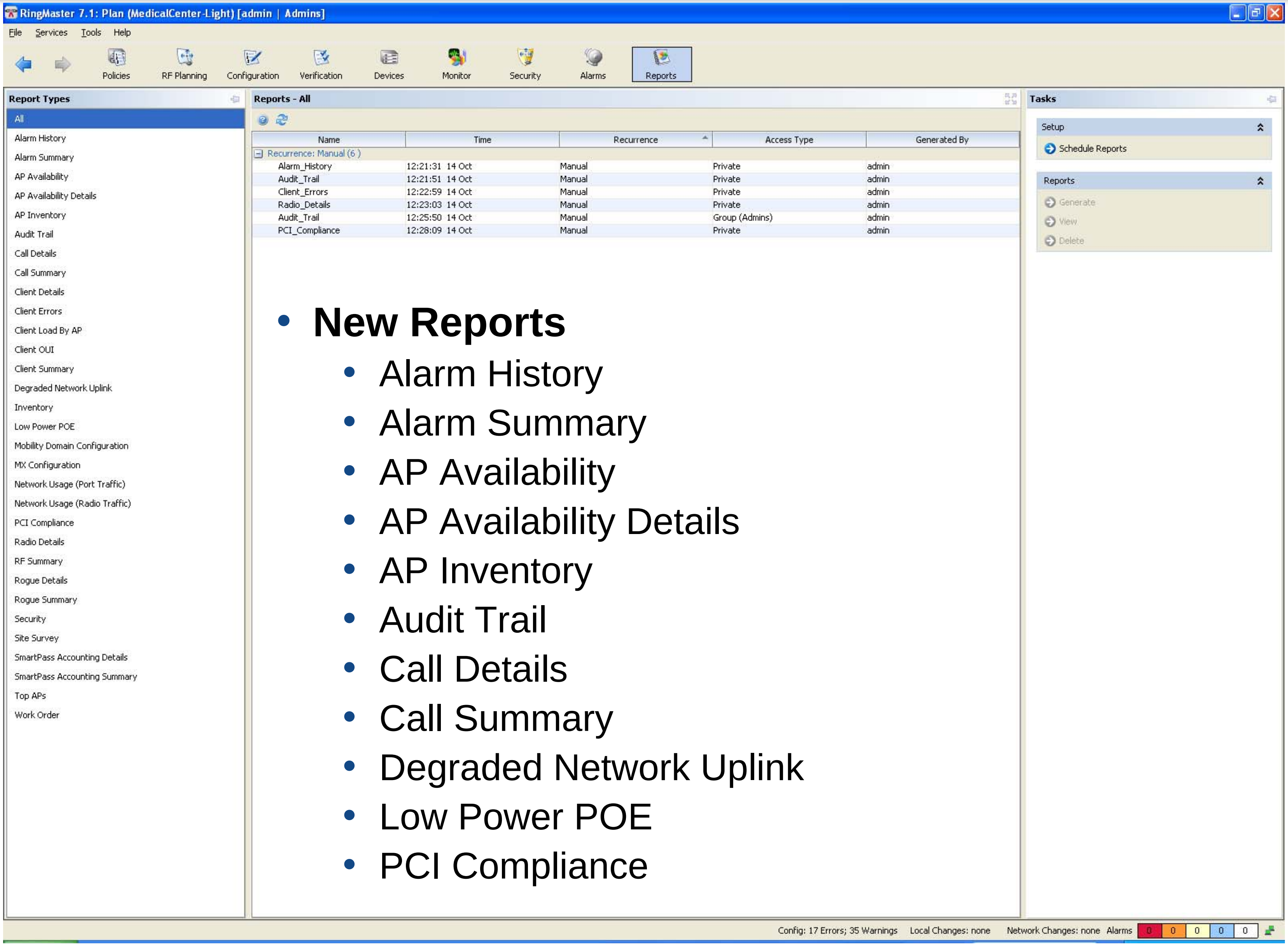
Maximum Packet Size (bytes): 4096

Timeout (s): 5

Retry Count: 2

- **Audit Trail settings**
  - Local auditing is enabled by default
  - External auditing to a RADIUS server may also be enabled
  - Use the new Audit Trail report to view the entries

Enhanced Reports



Report Types

- All
- Alarm History
- Alarm Summary
- AP Availability
- AP Availability Details
- AP Inventory
- Audit Trail
- Call Details
- Call Summary
- Client Details
- Client Errors
- Client Load By AP
- Client OUI
- Client Summary
- Degraded Network Uplink
- Inventory
- Low Power POE
- Mobility Domain Configuration
- MX Configuration
- Network Usage (Port Traffic)
- Network Usage (Radio Traffic)
- PCI Compliance
- Radio Details
- RF Summary
- Rogue Details
- Rogue Summary
- Security
- Site Survey
- SmartPass Accounting Details
- SmartPass Accounting Summary
- Top APs
- Work Order

Reports - All

Name	Time	Recurrence	Access Type	Generated By
⊟ Recurrence: Manual (6)				
Alarm_History	12:21:31 14 Oct	Manual	Private	admin
Audit_Trail	12:21:51 14 Oct	Manual	Private	admin
Client_Errors	12:22:59 14 Oct	Manual	Private	admin
Radio_Details	12:23:03 14 Oct	Manual	Private	admin
Audit_Trail	12:25:50 14 Oct	Manual	Group (Admins)	admin
PCI_Compliance	12:28:09 14 Oct	Manual	Private	admin

Tasks

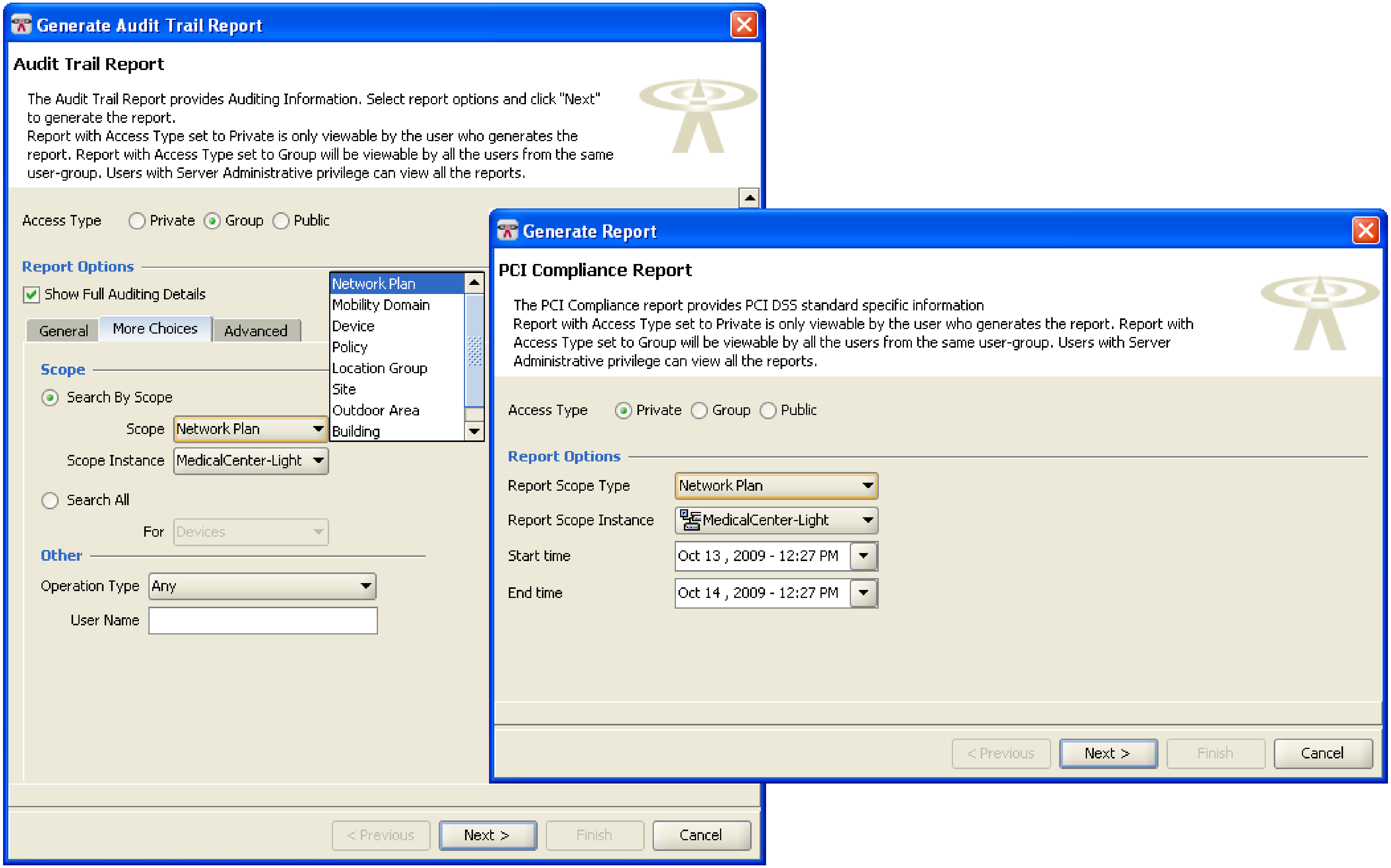
Setup
- Schedule Reports

Reports
- Generate
- View
- Delete

Config: 17 Errors; 35 Warnings Local Changes: none Network Changes: none Alarms 0 0 0 0 0

- **New Reports**
  - Alarm History
  - Alarm Summary
  - AP Availability
  - AP Availability Details
  - AP Inventory
  - Audit Trail
  - Call Details
  - Call Summary
  - Degraded Network Uplink
  - Low Power POE
  - PCI Compliance

Enhanced Reports



Generate Audit Trail Report

Audit Trail Report

The Audit Trail Report provides Auditing Information. Select report options and click "Next" to generate the report.
Report with Access Type set to Private is only viewable by the user who generates the report. Report with Access Type set to Group will be viewable by all the users from the same user-group. Users with Server Administrative privilege can view all the reports.

Access Type ○ Private ● Group ○ Public

Report Options

☑ Show Full Auditing Details

General | More Choices | Advanced

Scope

● Search By Scope

Scope: Network Plan

Scope Instance: MedicalCenter-Light

○ Search All

For: Devices

Other

Operation Type: Any

User Name:

Generate Report

PCI Compliance Report

The PCI Compliance report provides PCI DSS standard specific information
Report with Access Type set to Private is only viewable by the user who generates the report. Report with Access Type set to Group will be viewable by all the users from the same user-group. Users with Server Administrative privilege can view all the reports.

Access Type ● Private ○ Group ○ Public

Report Options

Report Scope Type: Network Plan

Report Scope Instance: MedicalCenter-Light

Start time: Oct 13 , 2009 - 12:27 PM

End time: Oct 14 , 2009 - 12:27 PM

Other RingMaster Features

- Monitoring improvements
  - New SNMP traps
  - Top BW by client monitoring
- AP and Session scaling
  - 5,000 APs in a Cluster
  - 10,000 Sessions for MX-2800
- Other Features
  - Configurable RingMaster port
  - MX access control
    - Enable Password
    - Username/Password
  - Client Blacklist and countermeasures enhancements
  - Server certificate management
  - Configurable MX management port

Ringmaster Global v7.1

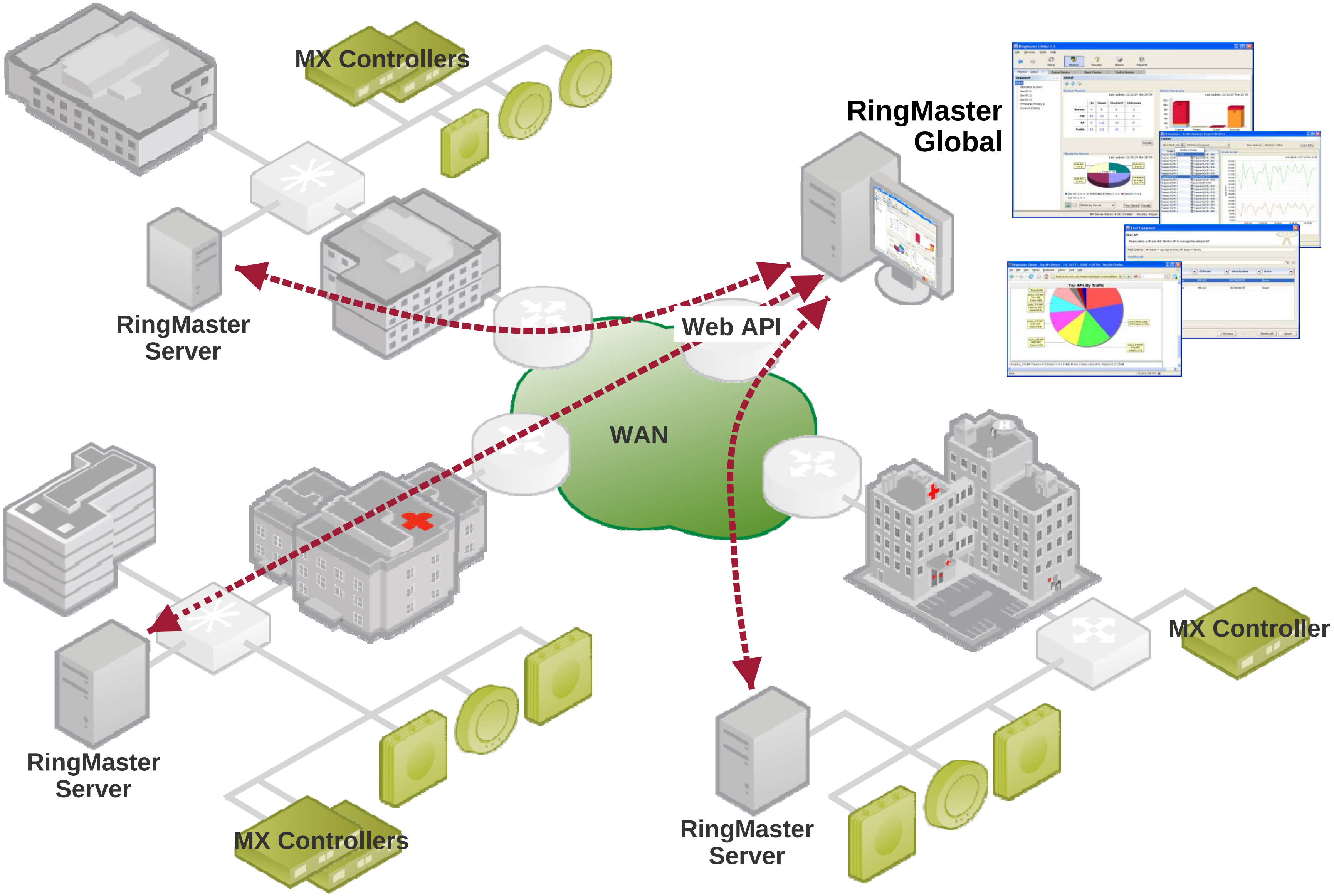
RingMaster Global (RMG) Overview

- Centralized Management for Large-scale Implementations
  - Manager of Managers – single Management Console for:
    - Up to 20 RingMaster servers
    - Up to 100,000 APs

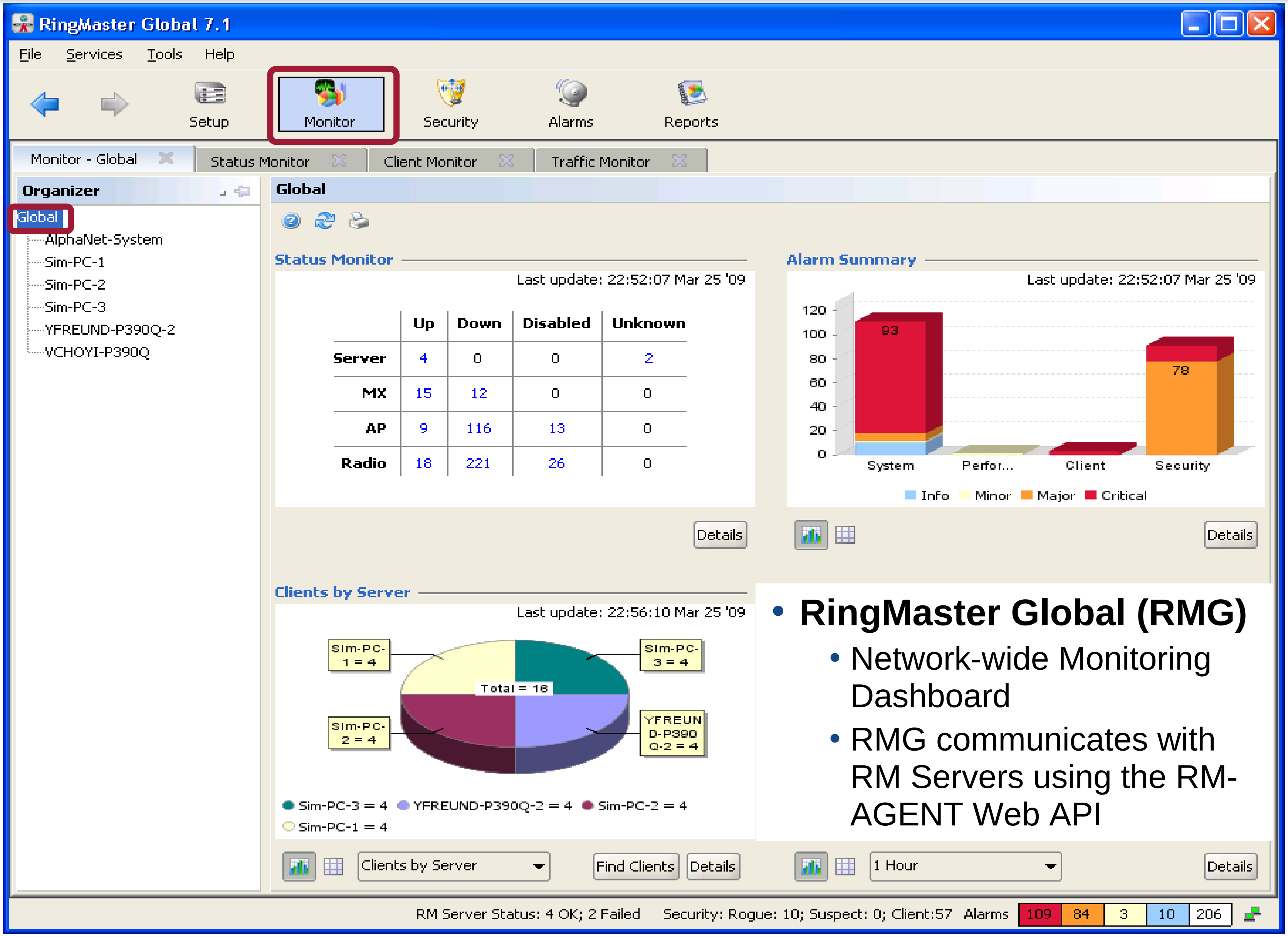
    Note: RingMaster Global communicates with RingMaster servers using the RingMaster Agent Web API

  - Single sign-on access control with optional AAA login
  - Network Wide Monitoring Dashboard, Search Capability and Reports
  - Licensing:
    - RMTS-GLOBAL
    - RMTS-GLOBAL-4
    - RMTS-GLOBAL-16
    - RMTS-GLOBAL-EVAL

RMG Management Architecture



Network-wide Monitoring



Status Monitor

Last update: 22:52:07 Mar 25 '09

	Up	Down	Disabled	Unknown
Server	4	0	0	2
MX	15	12	0	0
AP	9	116	13	0
Radio	18	221	26	0

Details

Alarm Summary

Last update: 22:52:07 Mar 25 '09

Clients by Server

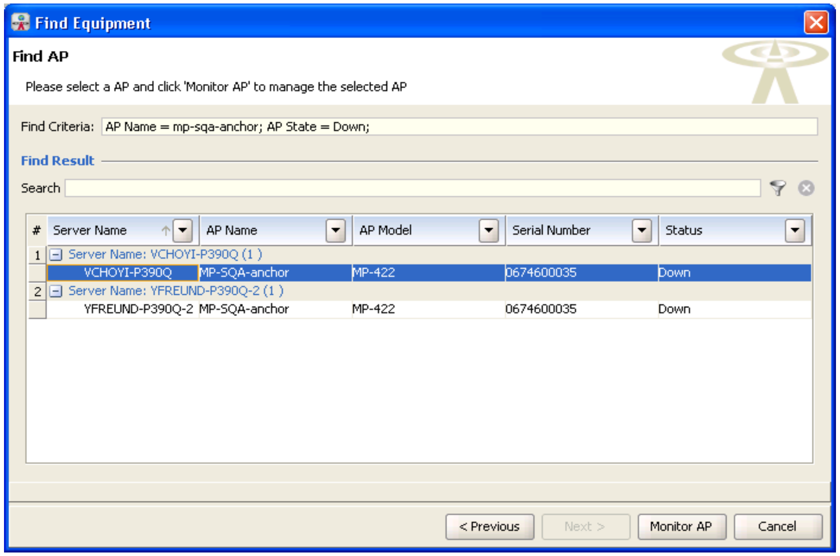
Last update: 22:56:10 Mar 25 '09

RM Server Status: 4 OK; 2 Failed Security: Rogue: 10; Suspect: 0; Client:57 Alarms 109 84 3 10 206

- **RingMaster Global (RMG)**
  - Network-wide Monitoring Dashboard
  - RMG communicates with RM Servers using the RM-AGENT Web API

Network-wide Search

- Network Wide Search Capability
  - Find Equipment (MXs/APs)
  - Find Locale (Site/Building/Floor)



Find Equipment

Find AP

Please select a AP and click 'Monitor AP' to manage the selected AP

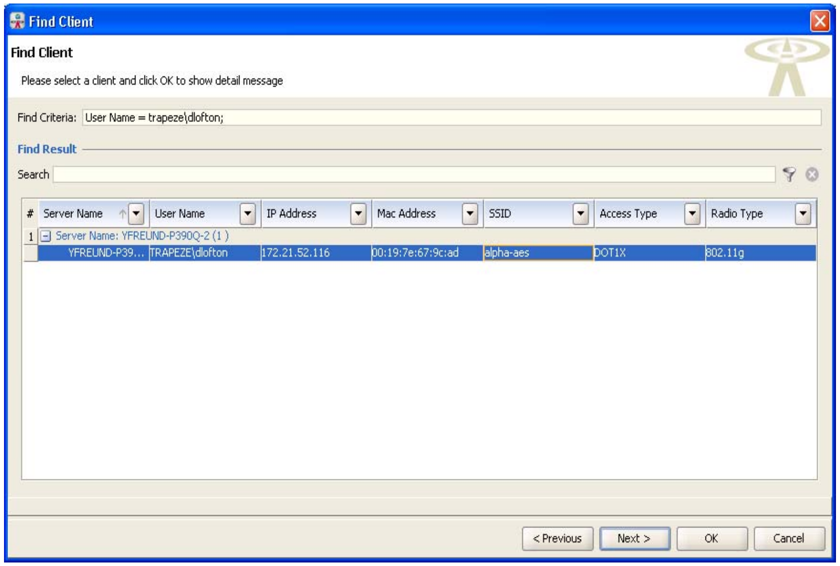
Find Criteria: AP Name = mp-sqa-anchor; AP State = Down;

Find Result

Search

#	Server Name	AP Name	AP Model	Serial Number	Status
1	Server Name: VCHOYI-P390Q (1)				
	VCHOYI-P390Q	MP-SQA-anchor	MP-422	0674600035	Down
2	Server Name: YFREUND-P390Q-2 (1)				
	YFREUND-P390Q-2	MP-SQA-anchor	MP-422	0674600035	Down

- Find Clients
- Launch RM UI for further diagnosis



Find Client

Find Client

Please select a client and click OK to show detail message

Find Criteria: User Name = trapeze\dlofton;

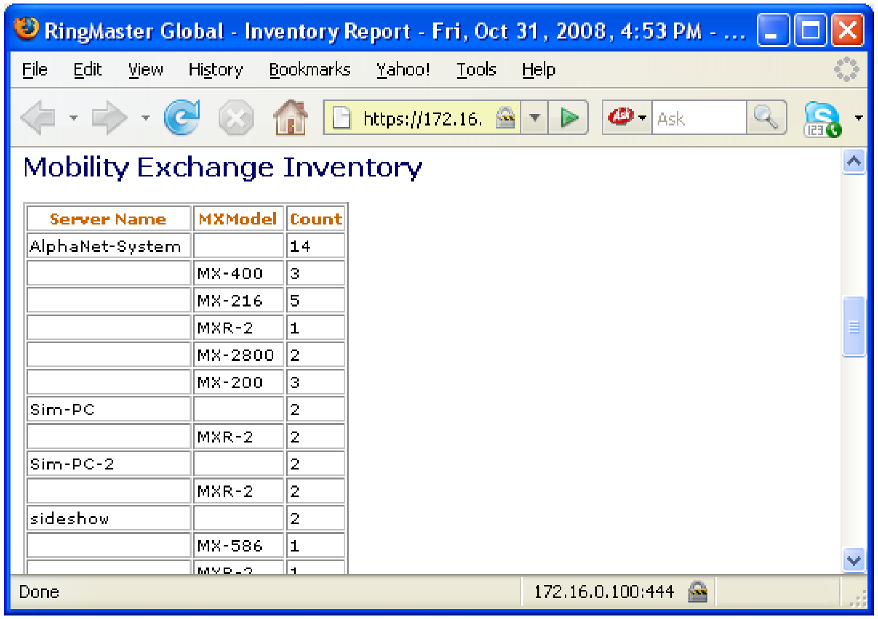
Find Result

Search

#	Server Name	User Name	IP Address	Mac Address	SSID	Access Type	Radio Type
1	Server Name: YFREUND-P390Q-2 (1)						
	YFREUND-P39...	TRAPEZE\dlofton	172.21.52.116	00:19:7e:67:9c:ad	alpha-aes	DOT1X	802.11g

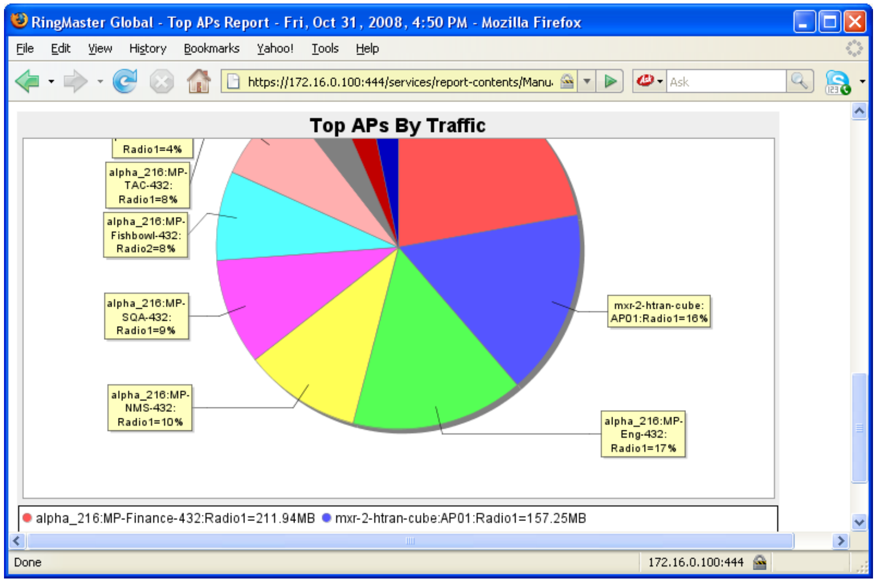
Network-wide Reporting

- Network Wide Reports


RingMaster Global - Inventory Report - Fri, Oct 31, 2008, 4:53 PM - ...
File Edit View History Bookmarks Yahoo! Tools Help
https://172.16.
Ask
Done
172.16.0.100:444

Mobility Exchange Inventory

Server Name	MXModel	Count
AlphaNet-System		14
	MX-400	3
	MX-216	5
	MXR-2	1
	MX-2800	2
	MX-200	3
Sim-PC		2
	MXR-2	2
Sim-PC-2		2
	MXR-2	2
sideshow		2
	MX-586	1
	MXR-2	1


RingMaster Global - Top APs Report - Fri, Oct 31, 2008, 4:50 PM - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://172.16.0.100:444/services/report-contents/Manu
Ask
Top APs By Traffic
Radio1=4%
alpha_216:MP-TAC-432: Radio1=8%
alpha_216:MP-Fishbowl-432: Radio2=8%
alpha_216:MP-SQA-432: Radio1=9%
alpha_216:MP-NMS-432: Radio1=10%
mxr-2-htran-cube: AP01:Radio1=16%
alpha_216:MP-Eng-432: Radio1=17%
● alpha_216:MP-Finance-432:Radio1=211.94MB ● mxr-2-htran-cube:AP01:Radio1=157.25MB
Done
172.16.0.100:444

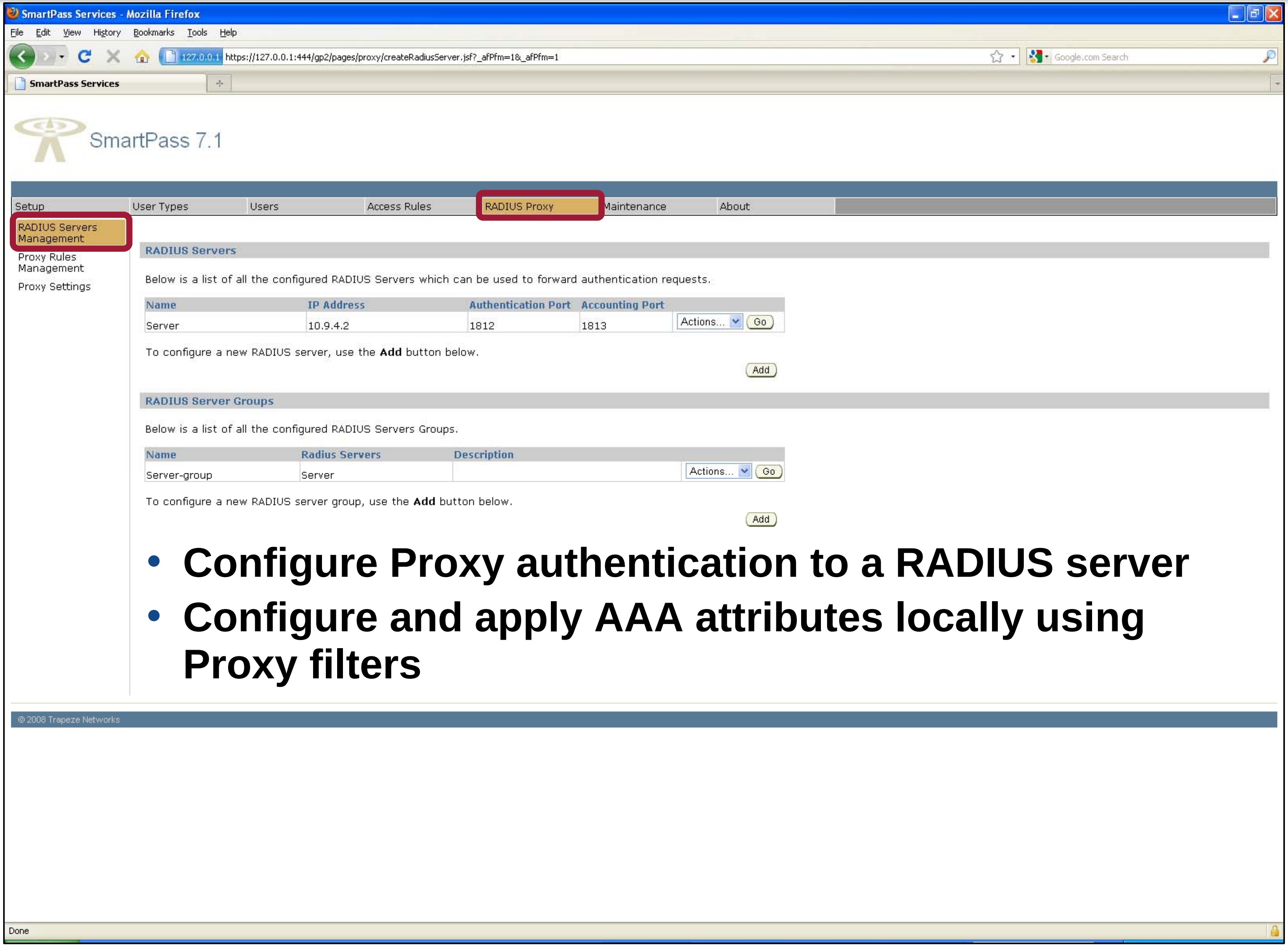
TRAPEZE NETWORKS
A BELDEN BRAND

SmartPass v7.1 Features & Enhancements

SmartPass v7.1 Topics

- RADIUS Proxy
- MAC Authentication
- Real time Session Monitoring
- Web API Enhancement
- Other Features
  - Linux installer
  - Server certificate import
  - User data export

RADIUS Proxy



SmartPass Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://127.0.0.1:444/gp2/pages/proxy/createRadiusServer.jsf?_afPfm=1&_afPfm=1
SmartPass Services
SmartPass 7.1
Setup
User Types
Users
Access Rules
RADIUS Proxy
Maintenance
About
RADIUS Servers Management
Proxy Rules Management
Proxy Settings
Done
© 2008 Trapeze Networks

RADIUS Servers

Below is a list of all the configured RADIUS Servers which can be used to forward authentication requests.

Name	IP Address	Authentication Port	Accounting Port	
Server	10.9.4.2	1812	1813	Actions... Go

To configure a new RADIUS server, use the **Add** button below.

Add

RADIUS Server Groups

Below is a list of all the configured RADIUS Servers Groups.

Name	Radius Servers	Description	
Server-group	Server		Actions... Go

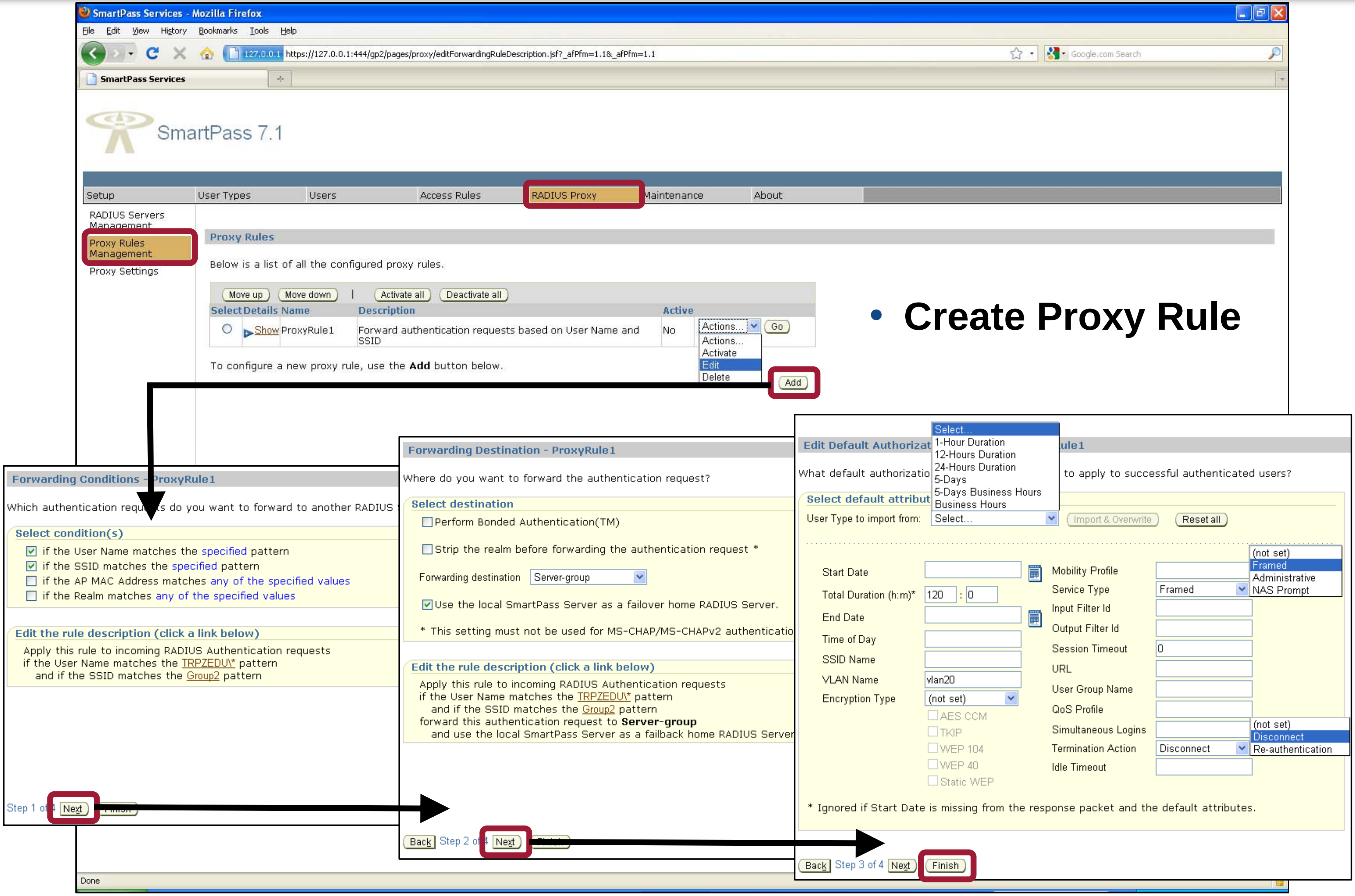
To configure a new RADIUS server group, use the **Add** button below.

Add

- **Configure Proxy authentication to a RADIUS server**
- **Configure and apply AAA attributes locally using Proxy filters**

RADIUS Proxy

- **Create Proxy Rule**


SmartPass Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://127.0.0.1:444/gp2/pages/proxy/editForwardingRuleDescription.jsf?_afPfm=1.1&_afPfm=1.1
SmartPass Services
SmartPass 7.1
Setup | User Types | Users | Access Rules | RADIUS Proxy | Maintenance | About
RADIUS Servers Management
Proxy Rules Management
Proxy Settings
Move up | Move down | Activate all | Deactivate all
Actions... | Activate | Edit | Delete
Go
Add
Next
Back
Finish
Done

Proxy Rules

Below is a list of all the configured proxy rules.

Select	Details	Name	Description	Active
○	Show	ProxyRule1	Forward authentication requests based on User Name and SSID	No

To configure a new proxy rule, use the **Add** button below.

Forwarding Conditions - ProxyRule1

Which authentication requests do you want to forward to another RADIUS

Select condition(s)

- ☑ if the User Name matches the specified pattern
- ☑ if the SSID matches the specified pattern
- ☐ if the AP MAC Address matches any of the specified values
- ☐ if the Realm matches any of the specified values

Edit the rule description (click a link below)

Apply this rule to incoming RADIUS Authentication requests
if the User Name matches the TRPZEDU* pattern
and if the SSID matches the Group2 pattern

Step 1 of 4

Forwarding Destination - ProxyRule1

Where do you want to forward the authentication request?

Select destination

- ☐ Perform Bonded Authentication(TM)
- ☐ Strip the realm before forwarding the authentication request *

Forwarding destination: Server-group

☑ Use the local SmartPass Server as a failover home RADIUS Server.

* This setting must not be used for MS-CHAP/MS-CHAPv2 authenticatio

Edit the rule description (click a link below)

Apply this rule to incoming RADIUS Authentication requests
if the User Name matches the TRPZEDU* pattern
and if the SSID matches the Group2 pattern
forward this authentication request to **Server-group**
and use the local SmartPass Server as a failback home RADIUS Server

Step 2 of 4

Edit Default Authorizat... ule1

What default authorizatio... to apply to successful authenticated users?

Select default attribut...

User Type to import from: Select... (Select... / 1-Hour Duration / 12-Hours Duration / 24-Hours Duration / 5-Days / 5-Days Business Hours / Business Hours)

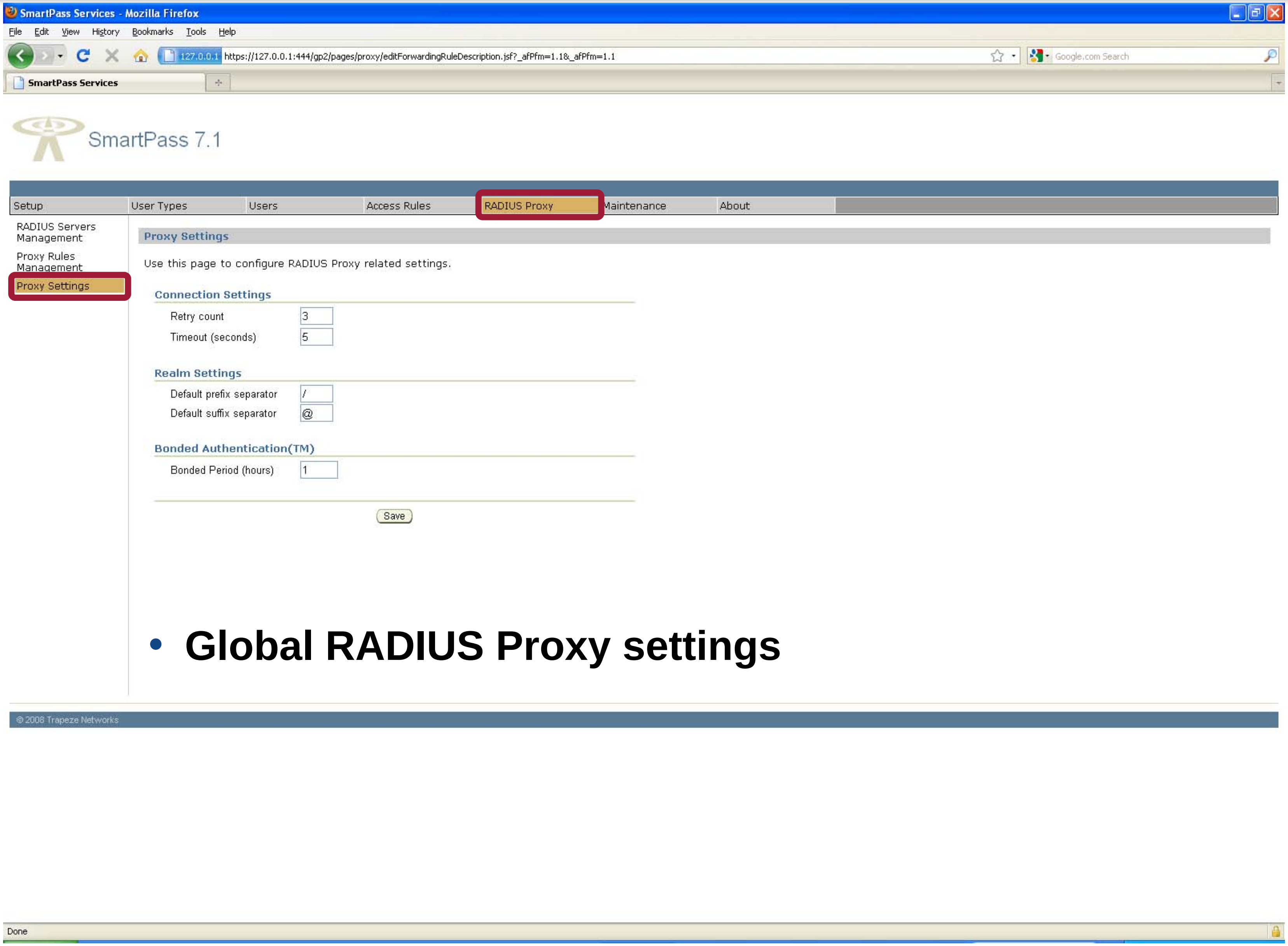
Import & Overwrite | Reset all

Start Date		Mobility Profile	
Total Duration (h:m)*	120 : 0	Service Type	Framed (not set / Framed / Administrative / NAS Prompt)
End Date		Input Filter Id	
Time of Day		Output Filter Id	
SSID Name		Session Timeout	0
VLAN Name	vlan20	URL	
Encryption Type	(not set)	User Group Name	
	☐ AES CCM	QoS Profile	
	☐ TKIP	Simultaneous Logins	
	☐ WEP 104	Termination Action	Disconnect (not set / Disconnect / Re-authentication)
	☐ WEP 40	Idle Timeout	
	☐ Static WEP		

* Ignored if Start Date is missing from the response packet and the default attributes.

Step 3 of 4

RADIUS Proxy


SmartPass Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
127.0.0.1 https://127.0.0.1:444/gp2/pages/proxy/editForwardingRuleDescription.jsf?_afPfm=1.1&_afPfm=1.1
Google.com Search
SmartPass Services
SmartPass 7.1
Setup
User Types
Users
Access Rules
RADIUS Proxy
Maintenance
About
RADIUS Servers Management
Proxy Rules Management
Proxy Settings
Save
© 2008 Trapeze Networks
Done

Proxy Settings

Use this page to configure RADIUS Proxy related settings.

Connection Settings

Retry count: 3

Timeout (seconds): 5

Realm Settings

Default prefix separator: /

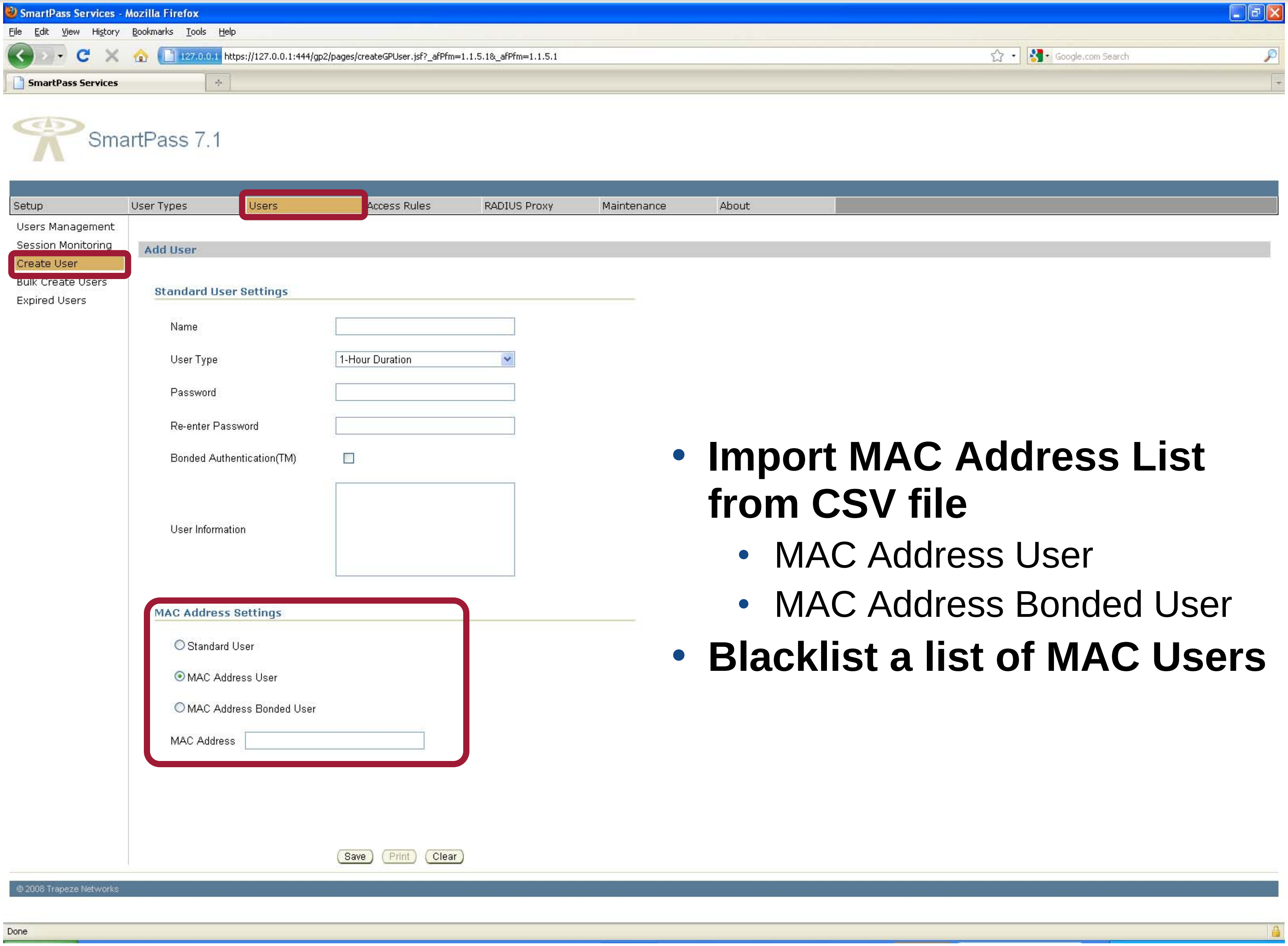
Default suffix separator: @

Bonded Authentication(TM)

Bonded Period (hours): 1

- **Global RADIUS Proxy settings**

MAC Authentication



Add User

Standard User Settings

Name	
User Type	1-Hour Duration
Password	
Re-enter Password	
Bonded Authentication(TM)	□
User Information	

MAC Address Settings

○ Standard User

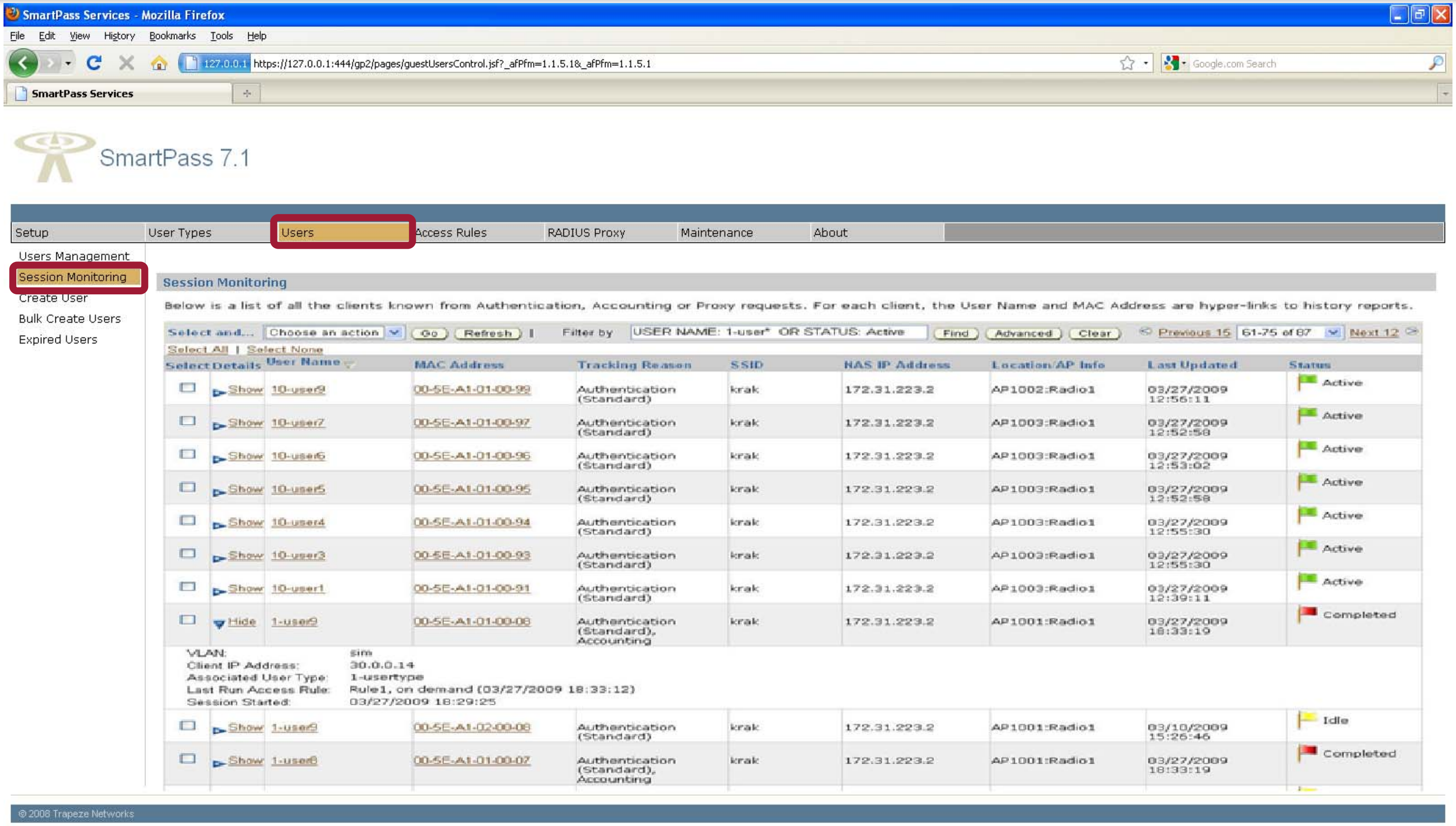
● MAC Address User

○ MAC Address Bonded User

MAC Address

- **Import MAC Address List from CSV file**
  - MAC Address User
  - MAC Address Bonded User
- **Blacklist a list of MAC Users**

Session Monitoring



Session Monitoring

Below is a list of all the clients known from Authentication, Accounting or Proxy requests. For each client, the User Name and MAC Address are hyper-links to history reports.

Filter by: USER NAME: 1-user* OR STATUS: Active

Select	Details	User Name	MAC Address	Tracking Reason	SSID	NAS IP Address	Location/AP Info	Last Updated	Status
□	Show	10-user9	00-5E-A1-01-00-99	Authentication (Standard)	krak	172.31.223.2	AP1002:Radio1	03/27/2009 12:56:11	Active
□	Show	10-user7	00-5E-A1-01-00-97	Authentication (Standard)	krak	172.31.223.2	AP1003:Radio1	03/27/2009 12:52:58	Active
□	Show	10-user6	00-5E-A1-01-00-96	Authentication (Standard)	krak	172.31.223.2	AP1003:Radio1	03/27/2009 12:53:02	Active
□	Show	10-user5	00-5E-A1-01-00-95	Authentication (Standard)	krak	172.31.223.2	AP1003:Radio1	03/27/2009 12:52:58	Active
□	Show	10-user4	00-5E-A1-01-00-94	Authentication (Standard)	krak	172.31.223.2	AP1003:Radio1	03/27/2009 12:55:30	Active
□	Show	10-user3	00-5E-A1-01-00-93	Authentication (Standard)	krak	172.31.223.2	AP1003:Radio1	03/27/2009 12:55:30	Active
□	Show	10-user1	00-5E-A1-01-00-91	Authentication (Standard)	krak	172.31.223.2	AP1003:Radio1	03/27/2009 12:39:11	Active
□	Hide	1-user9	00-5E-A1-01-00-08	Authentication (Standard), Accounting	krak	172.31.223.2	AP1001:Radio1	03/27/2009 18:33:19	Completed
VLAN: Client IP Address: Associated User Type: Last Run Access Rule: Session Started:	sim 30.0.0.14 1-usertype Rule1, on demand (03/27/2009 18:33:12) 03/27/2009 18:29:25								
□	Show	1-user9	00-5E-A1-02-00-08	Authentication (Standard)	krak	172.31.223.2	AP1001:Radio1	03/10/2009 15:26:46	Idle
□	Show	1-user8	00-5E-A1-01-00-07	Authentication (Standard), Accounting	krak	172.31.223.2	AP1001:Radio1	03/27/2009 18:33:19	Completed

- **Real Time Session Monitoring**
  - All sessions that SmartPass is tracking are displayed
  - Advanced Sorting and filtering capability

Done

Other Features

- Linux installer
  - SmartPass v7.1 now also installs on Linux platforms
  - Supported Linux versions are: Red Hat Enterprise Linux (RHEL) 5.0; SuSe 10.2
- Server certificate import
  - The new SmartPass v7.1 MR1 feature will now allow Administrators to replace the current server certificate with a web certificate.
  - Certificate recommendations:
    - The certificate should not be self-signed
    - Should support the Server extension
    - Should be issued to the SmartPass web-site address
    - Should not be expired
    - The root certificate should be trusted by the web-browser
- User data export
  - A new *'Export to CSV File'* item is available on the User Management Page
    - The exported CSV file includes: User names; Passwords (clear text); User Types; MAC Addresses (if available)

TRAPEZE NETWORKS
A BELDEN BRAND

Trapeze Networks Education Services

USA: Steven Elliott, Training Manager
+1 925 474 2261, selliott@trapezenetworks.com

EMEA: Pete Dahl, International Training Manager
+31 (0)35 6464 422, pdahl@trapezenetworks.com

Gerben Camp, Field Trainer EMEA
+31 (0)35 6464 427, gcamp@trapezenetworks.com

MSS v7.1 CLI Extracts

Advanced Licenses

```
#set license XXXX-XXXX-XXXX-XXXX-XXXX
  success: license accepted
```

Note: where *‘XXXX-XXXX-XXXX-XXXX-XXXX’* is the license activation key returned by the Trapeze Networks license server at

http://www.trapezenetworks.com/support/product_licenses/

```
#show license
  Serial Number    : XXXXXXXXXX

  Platform AP Count  : 32 access points are supported
  Licensed AP Count  : 96 additional access points
  Redundant AP Count : 64 access points are supported

  192 access points are supported

  Additional Features:

     Feature Description                Installed
     -------------------------------------------
     Adv Voice                             Yes
     Mesh/Bridging                         32
     High-Availability                     Yes
```

Voice / SIP Awareness

```
#set qos-profile <profile-name> cos <0..7>

#set qos-profile <profile-name> max-bw <kb/s>

#set qos-profile <profile-name> traffic-class voip-data cos <0..7>

#set qos-profile <profile-name> traffic-class voip-data max-bw <kb/s>

#set service-profile <profile-name> cac-voip-call <max-voip-calls>

#set radio-profile <profile-name> cac voice max-utilization <percentage>

#show session network qos-profile <profile-name>

#show sessions network sip <voice-details | statistics | verbose >

#show ap counters <apnum> radio <radionum> voice-details

#show service–profile <sp–name> cac
```

Clustering

- **AP Affinity**

```
#set mobility-domain ap-affinity-group address <ip> netmask <netmask>

#set mobility-domain ap-affinity-group address <ip/masklen>

#clear mobility-domain ap-affinity-group address <ip> netmask <netmask>

#clear mobility-domain ap-affinity-group address <ip/masklen>

#show mobility-domain ap-affinity-groups
```

- **Hitless Software Upgrade/Downgrade**

```
#show cluster upgrade

#upgrade cluster [force]
```

- **AP Status**

```
# Show ap status <options> cluster [member-ip]
```

Options: `apnum, boot-state, ip, mac, model, names, verbose`

AP to AP Tunneling

```
#set ap apnum tunnel-affinity affinity

#set ap auto tunnel-affinity affinity

#set vlan-profile <vp-name> vlan <vlan-name> [mode <overlay|local-switching>]

#set ap <apnum> local-switching mode enable [vlan-profile <name>]

#show ap config

#show tunnel ap

#show roaming vlan

#show ap vlan

#show vlan-profile
```

LDAP ‘set’ Commands

```
#set ldap server server-name [ address ip-address] { [auth-port port number ]
  [timeout seconds ] [deadtime minutes] [bind-mode [simple-auth|sasl-md5]]
  [fdqn dns-name] [mac-addr-format [hyphens|colons|one-hyphen-raw]] [base-dn
  basednstring] }

#set ldap server group <name_group> <server_1> {[server_2 … server_4]]

#set ldap server group <name_group> load-balance [enable|disable]

#set authentication [web|mac] [ssid ssid_name | wired] <user_glob>
  <ldap_group1> { [ldap_group2] [ldap_group3] [ldap_group4] } | local

#set authentication [admin|console] user_glob ldap_group1 { [ldap_group2]
  [ldap_group3] [ldap_group4] } | local
```

LDAP ‘set’ and ‘show’ Commands

```
#set ldap deadtime <minutes_num>

#set ldap timeout <seconds_num>

#set ldap auth-port <port_num>

#set ldap bind-mode [ simple-auth | sasl-md5]

#set ldap mac-addr-format [hyphens|colons|one-hyphen-raw]

#set ldap base-dn <base_dn_string>

#ldap-ping [server | group] <ldap_server_name> login <user_id> password
  <password>

#show ldap – displays all of the above LDAP settings
```

LDAP ‘clear’ Commands

```
#clear ldap server <server-name>

#clear ldap server group <name_group>

#clear authentication [web|mac] [ssid ssid_name | wired] <user_glob>

#clear authentication [admin|console] <user_glob>

#clear ldap deadtime

#clear ldap timeout

#clear ldap auth-port

#clear ldap bind-mode

#clear ldap mac-addr-format

#clear ldap base-dn
```

Command Auditing

```
#Set accounting

#Clear accounting
```

- No changes to show commands
- Radius STOP accounting record send for each logged command with the following attributes

Acct-Status-Type	Always set to STOP value
User-Name	TTY Name, No name, RM, SNMP or WV
Event-Timestamp	
Calling-Station-Id	IP Address of the user
Acct-Session-Id	Unique accounting session id for each entry
Acct-Multi-Session-Id	Unique value for same session id
NAS-Port	TTY port or connection port used
NAS-Port-Type	Type of connection
NAS-IP-Address	MX IP Address
NAS-Identifier	Always set to *'Trapeze'*

Command Auditing

- Radius STOP accounting record send for each logged command with the following attributes continued
  - Trapeze-Audit String VSA Containing the audit info
    - ***‘cmd=’:*** the Logged CLI command
    - ***‘xml=’:*** the Logged XML command
    - ***‘status=’:*** command/transaction execution status *‘Success’* or *‘Fail’*
    - ***‘version=’:*** MSS Version string
    - ***‘platform=’:*** MSS Platform string
    - ***‘serial=’:*** the serial number of the platform
  - Long Audit information is fragmented into multiple accounting audit packets
    - ***‘fragment=’:*** sequence number indicates the sequence number of the fragments

AP LED Control

```
#set ap apnum led-mode { auto|static|off}

#set ap <apnum range> led-mode {auto|static|off}

#set ap auto led-mode {auto|static|off}

#show ap config
```

- Now displays the led-mode

Enhancement to Dynamic RF Blacklist

```
#set rfdetect black-list dynamic {enable | disable }

#set rfdetect black-list dynamic duration <seconds>

#Set rfdetect black-list <mac> {dynamic}

#show rfdetect black-list reflects cluster-wide information

#clear rfdetect black-list
```

802.1x TKIP/CCMP Rekey Timers

```
#set/clear dot1x unicast-rekey-period [30..86400]

#set/clear dot1x multicast-rekey-period [30..86400]

#set dot1x unicast-rekey [enable|disable]

#set dot1x multicast-rekey [enable|disable]

#show dot1x config
```